vSpere IaaS 制御プレーンの概念と計画

Update 3
VMware vSphere 8.0
VMware vCenter 8.0
VMware ESXi 8.0

vmware
by Broadcom

VMware by Broadcom の Web サイトで最新の技術ドキュメントを確認できます

https://docs.vmware.com/jp/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目次

vSphere IaaS 制御プレーンの概念と計画

この『vSphere IaaS 制御プレーンの概念と計画』ガイドでは、vSphere IaaS control plane（旧称は vSphere with Tanzu）の主な概念とアーキテクチャ、および vSphere 環境が満たす必要のある要件について説明します。この情報を確認することにより、vSphere クラスタで vSphere IaaS control plane を有効にし、Tanzu Kubernetes Grid クラスタ、vSphere ポッド、および仮想マシン サービスを使用して作成された仮想マシンでワークロードを実行できます。

対象読者

この情報は、vSphere で vSphere IaaS control plane を有効にするための要件およびプラットフォームの主な概念とアーキテクチャについて理解する必要のある vSphere 管理者および DevOps エンジニアを対象としています。

更新情報

『vSphere IaaS 制御プレーンの概念と計画』は、製品のリリースごとに、または必要に応じて更新されます。

『vSphere IaaS 制御プレーンの概念と計画』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2024 年 4 月 18 日	新しいソリューションのライセンス情報を更新しました。vSphere IaaS control plane のライセンスを参照してください。
2024 年 2 月 29 日	クラウドに関するコンテンツを追加しました。NSX Advanced Load Balancer コンポーネントを参照してください。
2024 年 2 月 7 日	「スーパーバイザー ネットワーク」のリンクを更新しました。
2023 年 12 月 13 日	NSX の要件を更新し、vSphere クラスタに NSX トランスポート ノードとして参加しているすべての ESXi ホストの準備について注記を追加しました。NSX でのゾーン スーパーバイザー の要件と NSX を使用したクラスタ スーパーバイザー のデプロイの要件を参照してください。
2023 年 9 月 29 日	HAProxy をデプロイする際のロード バランサの要件を更新しました。HA プロキシ ロード バランサを使用したゾーン スーパーバイザー デプロイの要件と Distributed Switch ネットワークと HAProxy ロード バランサを使用したクラスタ スーパーバイザー のデプロイの要件を参照してください
2023 年 9 月 21 日	NSX と NSX Advanced Load Balancer を使用した スーパーバイザー ネットワークに関する内容を追加しました。vSphere IaaS control plane のユーザー ロールとワークフローとスーパーバイザー ネットワークを参照してください。
2023 年 8 月 3 日	マイナー改訂。
2023 年 6 月 30 日	■ 「スーパーバイザー ゾーンおよびクラスタのデプロイ」に物理サイト間での vSphere Zone の分布に関する記述を追加しました。
2023 年 6 月 9 日	■ 「vSphere IaaS control plane セキュリティ」に次の記述を追加しました。 同じ暗号化モデルは、各 Tanzu Kubernetes Grid クラスタの制御プレーンにインストールされているデータベース (etcd) 内のデータに適用されます。 ■ パーシステント ボリュームで Storage vMotion がサポートされないという記述を追加しました。スーパーバイザーと vSphere ストレージの統合方法と Tanzu Kubernetes Grid クラスタのストレージを参照してください。 ■ 「5 章 ゾーン スーパーバイザー デプロイの要件」と「6 章 クラスタ スーパーバイザー デプロイの要件」のベスト プラクティスとして、管理ドメインとワークロード ドメインを分離するための推奨事項を追加しました。
2023 年 6 月 2 日	■ 『NSX Reference Design Guide』へのリンクを追加しました。NSX でのゾーン スーパーバイザー の要件と NSX を使用したクラスタ スーパーバイザー のデプロイの要件を参照してください。 ■ マイナー更新。
2023 年 5 月 30 日	■ NSX のデプロイのための GENEVE カプセル化のサポート要件を追加しました。「NSX を使用したゾーン スーパーバイザーの要件」および「NSX を使用したクラスタ スーパーバイザーのデプロイの要件」を参照してください。 ■ マイナー更新。
2023 年 5 月 12 日	vSphere IaaS control plane 環境を vSphere 8.0 より前のバージョンからアップグレードして vSphere Zone を使用する場合は、新しい 3 ゾーン スーパーバイザー を作成する必要があるという注記を追加しました。5 章 ゾーン スーパーバイザー デプロイの要件を参照してください。

リビジョン	説明
2023 年 5 月 9 日	■ 個別のトピック「vSphere 名前空間 について」を追加しました。 ■ 「vSphere IaaS control plane ID とアクセスの管理」の内容を更新しました。 ■ vSphere ポッド は NSX ネットワーク スタックでのみサポートされるという注記を追加しました。vSphere ポッド についてを参照してください。
2023 年 5 月 1 日	マイナー改訂。
2023 年 4 月 18 日	vSphere 8 Update 1 リリースの一般的な更新。

vSphere IaaS control plane の概念

1

vSphere IaaS control plane を使用すると、vSphere クラスタを vSphere の専用のリソース プールで Kubernetes ワークロードを実行するためのプラットフォームに変換できます。vSphere IaaS control plane を vSphere クラスタで有効にすると、Kubernetes 制御プレーンがハイパーバイザー レイヤーに直接作成されます。vSphere ポッド をデプロイして Kubernetes コンテナを実行することができます。また、VMware Tanzu™ Kubernetes Grid™ を使用してアップストリームの Kubernetes クラスタを作成し、これらのクラスタ内でアプリケーションを実行することもできます。

次のトピックを参照してください。

- vSphere IaaS control plane について
- vSphere 名前空間 について
- vSphere IaaS control plane のユーザー ロールとワークフロー
- vSphere IaaS control plane による vSphere 環境の変革
- vSphere IaaS control plane のライセンス
- vSphere IaaS control plane ID とアクセスの管理
- vSphere IaaS control plane セキュリティ

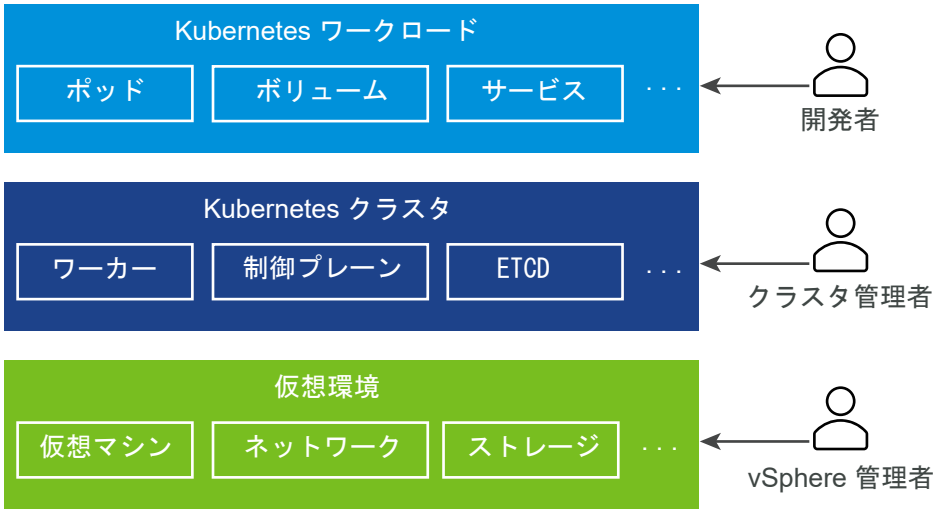
vSphere IaaS control plane について

vSphere IaaS control plane を使用すると、vSphere を、Kubernetes ワークロードをハイパーバイザー レイヤーでネイティブに実行するためのプラットフォームに変換できます。vSphere クラスタで vSphere IaaS control plane を有効にすると、Kubernetes ワークロードを ESXi ホストで直接実行し、専用の名前空間（vSphere 名前空間）内にアップストリーム Kubernetes クラスタを作成する機能が提供されます。

現在のアプリケーション スタックについての課題

現在の分散システムは、一般に多数の Kubernetes ポッドと仮想マシンを実行する複数のマイクロサービスから構成されています。vSphere IaaS control plane に基づかない典型的なスタックは、各仮想マシン内に Kubernetes インフラストラクチャがデプロイされた基盤となる仮想環境と、これらの仮想マシンでそれぞれ実行される Kubernetes ポッドで構成されます。スタックの各部分は、アプリケーション開発者、Kubernetes クラスタ管理者、および vSphere 管理者の 3 種類のロールによって操作されます。

図 1-1. 現在のアプリケーション スタック



各ロールは、互いの環境を可視化または制御できません。

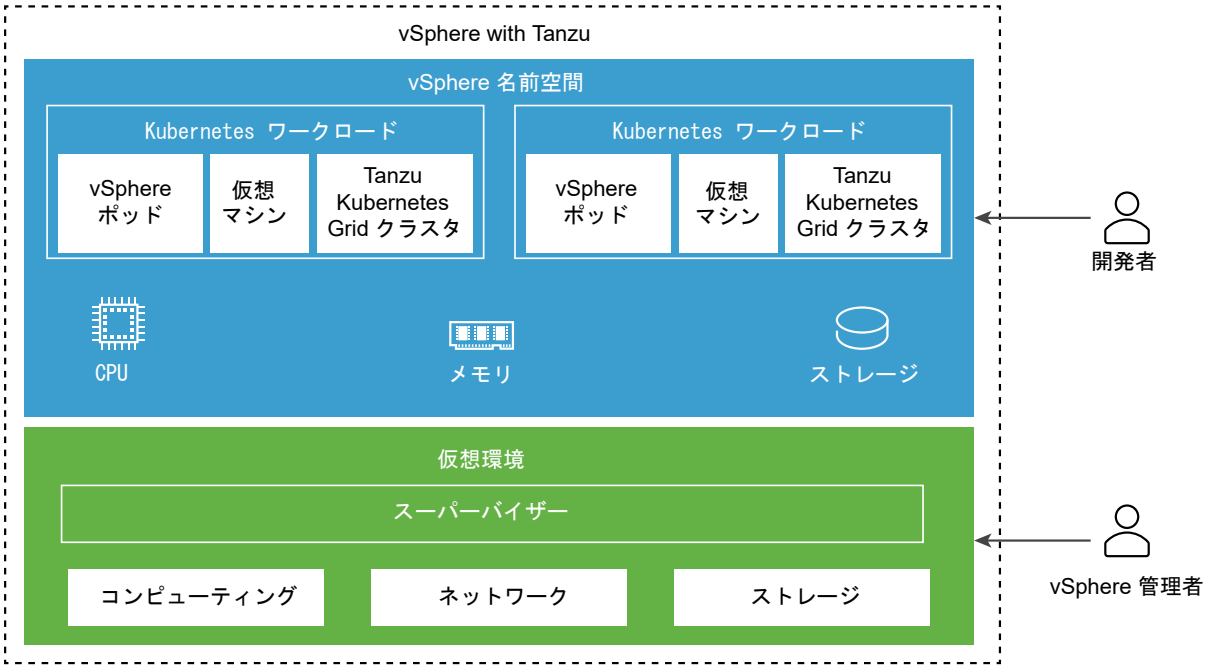
- アプリケーション開発者は、Kubernetes ポッドの実行と、Kubernetes ベースのアプリケーションのデプロイおよび管理を行うことができます。数百のアプリケーションを実行しているスタック全体は可視化できません。
- DevOps エンジニアまたはクラスタ管理者は、Kubernetes インフラストラクチャのみを制御することができます。仮想環境を管理または監視することや、リソース関連の問題やその他の問題を解決することはできません。
- vSphere 管理者は、基盤となる仮想環境を完全に制御できますが、Kubernetes インフラストラクチャ、仮想環境内でのさまざまな Kubernetes オブジェクトの配置、およびそれらのオブジェクトによるリソースの使用を可視化することはできません。

3 つのすべてのロール間の通信が必要になるため、スタック全体の操作は困難になる可能性があります。また、スタックの異なるレイヤーが統合されていないことが問題となる場合もあります。たとえば、Kubernetes スケジューラには vCenter Server インベントリに対する可視性がないため、ポッドをインテリジェントに配置することができません。

vSphere IaaS control plane を使用するメリット

vSphere IaaS control plane は、Kubernetes 制御プレーンをハイパーバイザー レイヤーに直接作成します。vSphere 管理者は、既存の vSphere クラスタで vSphere IaaS control plane を有効にし、このクラスタに含まれている ESXi ホスト内に Kubernetes レイヤーを作成します。vSphere IaaS control plane に対して有効になっている vSphere クラスタは、スーパーバイザー と呼ばれます。

図 1-2. vSphere IaaS control plane



ハイパーバイザー レイヤーに Kubernetes 制御プレーンがあると、vSphere で次の機能が実現します。

- vSphere 管理者は、vSphere 名前空間 という スーパーバイザー 上の名前空間を作成し、指定された容量のメモリ、CPU、ストレージを使用して名前空間を構成することができます。構成した vSphere 名前空間 は、DevOps エンジニアに提供します。
- DevOps エンジニアは、同じプラットフォームの Kubernetes ワークロードを、vSphere 名前空間 内の共有リソース プールで実行できます。Tanzu Kubernetes Grid を使用して作成された複数のアップストリーム Kubernetes クラスタをデプロイおよび管理できます。Kubernetes コンテナは、vSphere ポッド と呼ばれる特別なタイプの仮想マシン内の スーパーバイザー に直接デプロイすることもできます。通常の仮想マシンをデプロイすることもできます。
- vSphere 管理者は、vSphere Client を使用して、vSphere ポッド、仮想マシン、および Tanzu Kubernetes Grid クラスタを管理および監視できます。
- vSphere 管理者は、異なる名前空間内で実行されている vSphere ポッド、仮想マシン、Tanzu Kubernetes Grid クラスタ、環境内でのそれらの配置、およびそれらのオブジェクトによるリソースの使用方法を完全に可視化できます。

ハイパーバイザー レイヤーで Kubernetes を実行していると、vSphere 管理者と DevOps チームの両方のロールが同じオブジェクトを操作するため、共同作業も容易になります。

ワークロードについて

vSphere IaaS control plane では、ワークロードとは次のいずれかの方法でデプロイされたアプリケーションを指します。

- vSphere ポッド 内で実行されているコンテナで構成されるアプリケーション。

- 仮想マシン サービスを介してプロビジョニングされるワークロード。
- Tanzu Kubernetes Grid を使用してデプロイされた Tanzu Kubernetes Grid クラスタ。
- Tanzu Kubernetes Grid クラスタ内で実行されるアプリケーション。

vSphere Zone とは

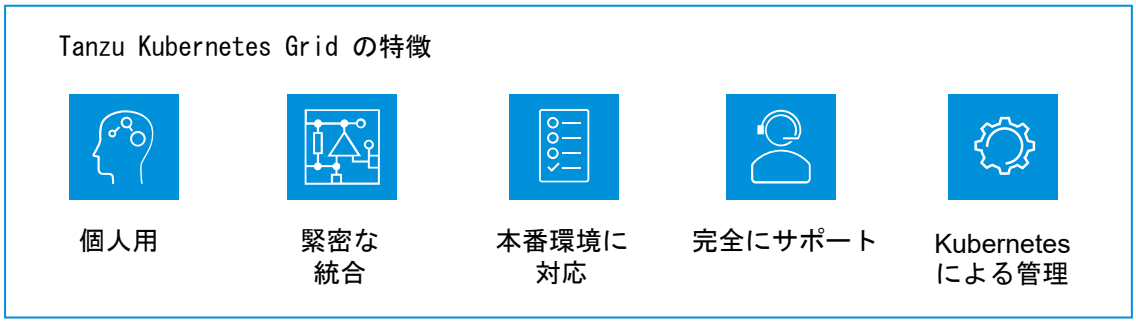
vSphere Zone は、vSphere IaaS control plane にデプロイされたワークロードのクラスタレベルの障害に対し、高可用性を提供します。vSphere 管理者は、vSphere Client に vSphere Zone を作成してから、vSphere クラスタをゾーンにマッピングします。ゾーンを使用して、vSphere IaaS control plane 環境に スーパーバイザー をデプロイします。

クラスタレベルの高可用性を実現するために、スーパーバイザー を 3 つの vSphere Zone にデプロイできます。または、スーパーバイザー を単一の vSphere クラスタにデプロイすることもできます。これにより、vSphere Zone が自動的に作成され、クラスタにマッピングされます。すでにゾーンにマッピングされているクラスタを使用することもできます。詳細については、『スーパーバイザー アーキテクチャ』および『スーパーバイザー ゾーンおよびクラスタのデプロイ』を参照してください。

Tanzu Kubernetes Grid クラスタについて

Tanzu Kubernetes Grid クラスタは、VMware によってビルド、署名、およびサポートされている Kubernetes の完全なディストリビューションです。Tanzu Kubernetes Grid を使用することで、アップストリーム Tanzu Kubernetes Grid クラスタを スーパーバイザー 上にプロビジョニングして運用することができます。

Tanzu Kubernetes Grid によってプロビジョニングされる Tanzu Kubernetes Grid クラスタには、次の特性があります。



- Kubernetes の個人用インストール。Tanzu Kubernetes Grid では、vSphere で Tanzu Kubernetes Grid クラスタをプロビジョニングするために十分に考慮され、最適化されたデフォルト値が提供されています。Tanzu Kubernetes Grid を使用することで、通常エンタープライズ レベルの Kubernetes クラスタをデプロイおよび実行する際に必要になる時間と労力の削減が可能になります。
- vSphere インフラストラクチャとの統合。Tanzu Kubernetes Grid クラスタは、ストレージ、ネットワーク、認証などを含めて、vSphere Software-Defined Data Center (SDDC) スタックと緊密に統合されています。また、Tanzu Kubernetes Grid クラスタは、vSphere クラスタにマッピングされる スーパーバイザー 上に構築されます。緊密に統合されているため、他の製品と同様な操作方法で Tanzu Kubernetes Grid クラスタを実行することができます。

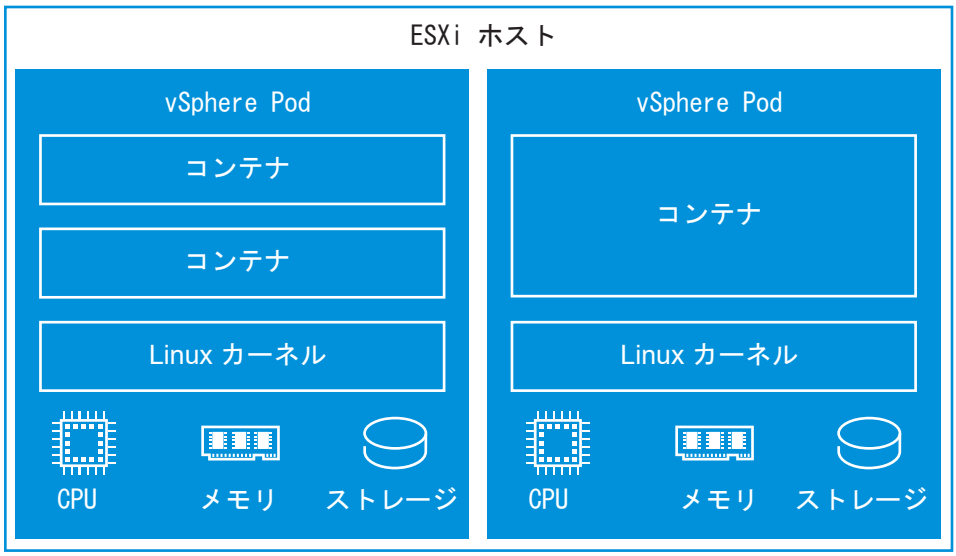
- 本番環境に対応。Tanzu Kubernetes Grid は、本番環境に対応した Tanzu Kubernetes Grid クラスタをプロビジョニングします。追加の設定を行う必要なく、本番環境のワークロードを実行できます。また、可用性を確保し、Kubernetes ソフトウェアのローリング アップグレードを可能にし、異なるバージョンの Kubernetes を別々のクラスタで実行することもできます。
- Kubernetes ワークロードの高可用性。3 つの vSphere Zone で構成される スーパーバイザー にデプロイされた Tanzu Kubernetes Grid クラスタは、vSphere クラスタ レベルの障害から保護されます。Tanzu Kubernetes Grid クラスタのワークロードと制御プレーン ノードは 3 つすべての vSphere Zone に分散されるため、その中で実行されている Kubernetes ワークロードの高可用性が確保されます。1 ゾーンの スーパーバイザー で実行されている Tanzu Kubernetes Grid クラスタは、vSphere HA を介して ESXi ホスト レベルの障害から保護されます。
- VMware による完全サポート。Tanzu Kubernetes Grid クラスタは、VMware が提供するオープンソースの Linux ベースを使用し、vSphere インフラストラクチャにデプロイされ、ESXi ホストで実行されます。ハイパーバイザーから Kubernetes クラスタに至るまで、スタックのどのレイヤーでも問題が発生した場合は、VMware がお客様のお問い合わせ先となります。
- Kubernetes による管理。Tanzu Kubernetes Grid クラスタは、Kubernetes クラスタである スーパーバイザー 上に構築されています。Tanzu Kubernetes Grid は、カスタム リソースを使用して vSphere 名前空間 で定義されます。Tanzu Kubernetes Grid クラスタをセルフサービスでプロビジョニングするには、使い慣れた kubectl コマンドと Tanzu CLI を使用します。ツールチェーン全体に整合性があるため、クラスタをプロビジョニングする場合でも、またはワークロードをデプロイする場合でも、同じコマンド、使い慣れた YAML、共通のワークフローを使用できます。

詳細については、3 章 Tanzu Kubernetes Grid アーキテクチャおよびコンポーネントおよび『vSphere IaaS 制御プレーンでの TKG サービスの使用』を参照してください。

vSphere ポッド について

vSphere IaaS control plane では、Kubernetes ポッドに相当する vSphere ポッド と呼ばれる構造が導入されています。vSphere ポッド は、1 つ以上の Linux コンテナを実行する占有量の小さい仮想マシンです。各 vSphere ポッド は、格納するワークロードに応じて正確にサイズ調整され、そのワークロードに対して明示的なリソース予約を保持します。これにより、ワークロードの実行に必要な量のストレージ、メモリ、および CPU リソースが正確に割り当てられます。vSphere ポッド は、ネットワーク スタックとして NSX を使用して構成された スーパーバイザー でのみサポートされます。

図 1-3. vSphere ポッド

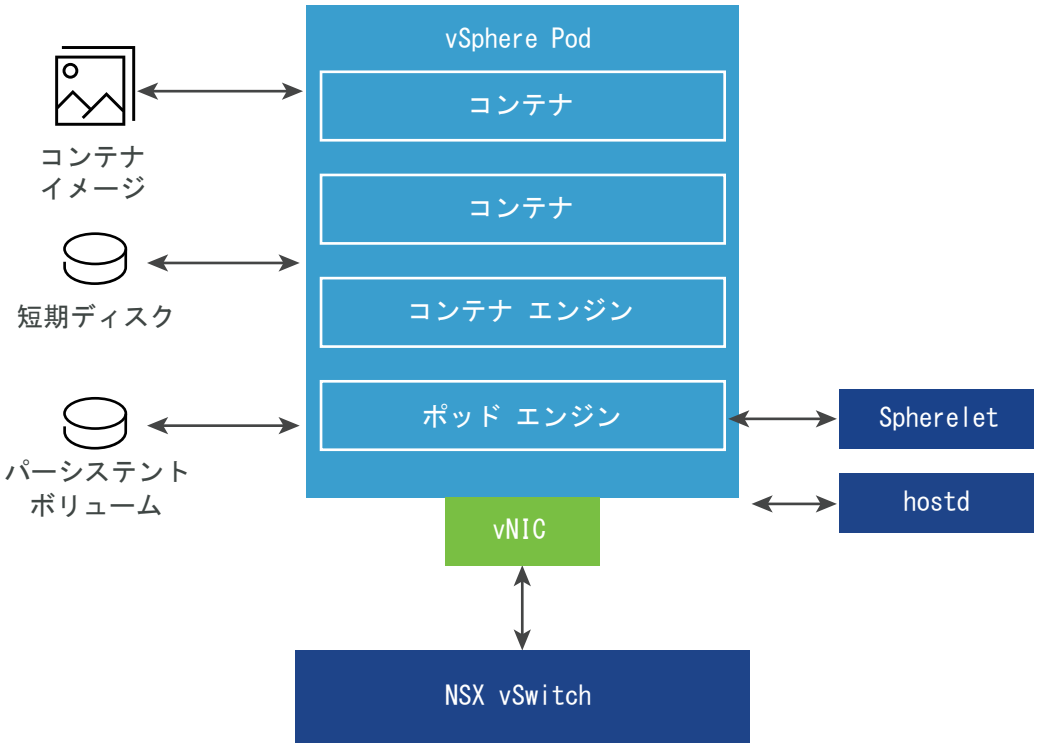


vSphere ポッド は vCenter Server 内のオブジェクトであり、ワークロードに対して次の機能を実現します。

- 高レベルの隔離。vSphere ポッド は、仮想マシンと同じ方法で隔離されます。各 vSphere ポッド には、Photon OS で使用されるカーネルに基づく独自の Linux カーネルがあります。vSphere ポッド では、ベアメタル構成と異なり、多くのコンテナでカーネルを共有することはありません。コンテナごとに一意の Linux カーネルがあります
- リソース管理。vSphere DRS により、スーパーバイザー 上の vSphere ポッド の配置が処理されます。
- 高パフォーマンス。vSphere ポッド では、仮想マシンと同じレベルのリソース隔離が実現するため、高速な起動時間と、コンテナの低オーバーヘッドを維持しながら、ノイジー ネイバー問題を回避できます。
- 診断。vSphere 管理者は、ワークロード上の vSphere で使用可能なすべての監視ツールおよびイントロスペクション ツールを使用できます。

vSphere ポッド は Open Container Initiative (OCI) と互換性があり、任意のオペレーティング システムのコンテナを実行できます（コンテナも OCI 互換の場合に限る）。

図 1-4. vSphere ポッド ネットワークおよびストレージ



vSphere ポッド では、格納するオブジェクトに応じて、短期 VMDK、パーシステント ボリューム VMDK、およびコンテナ イメージ VMDK の 3 種類のストレージを使用します。vSphere 管理者は、スーパーバイザー レベルでコンテナ イメージ キャッシュと短期 VMDK を配置するためのストレージ ポリシーを構成します。vSphere 名前空間 レベルでは、パーシステント ボリュームを配置するためのストレージ ポリシーを構成します。vSphere IaaS control plane におけるストレージの要件と概念の詳細については、ワークロードのパーシステント ストレージを参照してください。

ネットワークについては、vSphere ポッド と Tanzu Kubernetes Grid クラスタの仮想マシンは、NSX によって提供されるトポロジを使用します。詳細については、スーパーバイザー ネットワークを参照してください。

Spherelet は、各ホストで作成される追加のプロセスです。このプロセスは、ESXi に対してネイティブに移植された kubelet であり、このプロセスによって ESXi ホストは Kubernetes クラスタのメンバーになることができます。

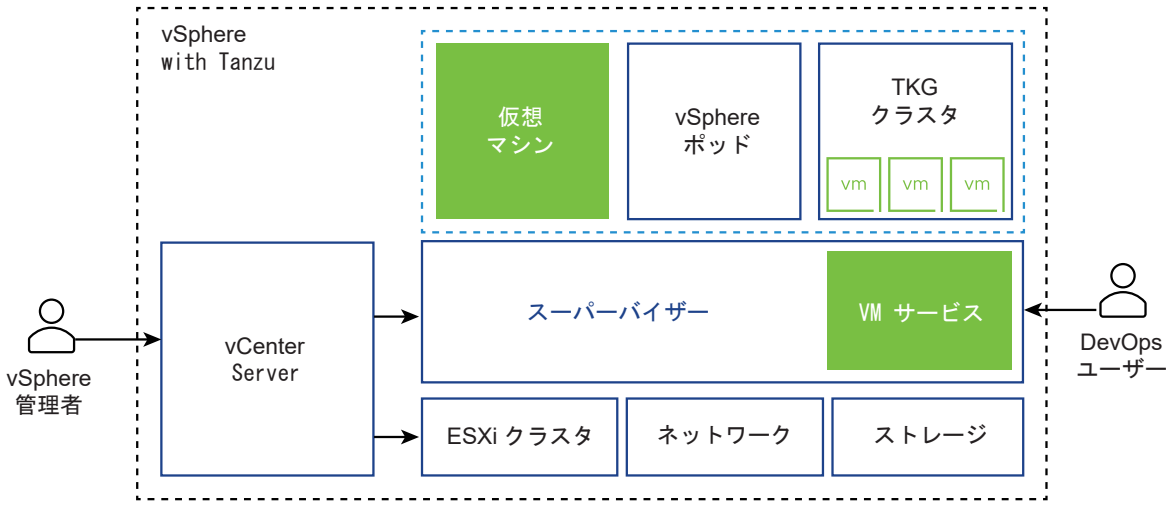
スーパーバイザー で vSphere ポッド を使用する方法については、『vSphere IaaS 制御プレーンのサービスとワークロード』ドキュメントの vSphere ポッドへのワークロードのデプロイを参照してください。

vSphere IaaS control plane での仮想マシンの使用

vSphere IaaS control plane で提供されている仮想マシン サービス機能を使用すると、DevOps エンジニアは一般的な共有 Kubernetes 環境でコンテナに加え、仮想マシンをデプロイして実行することができます。コンテナと仮想マシンの両方が同じ vSphere 名前空間 リソースを共有するため、単一の vSphere IaaS control plane インターフェイスを通して管理することができます。

仮想マシン サービスは、Kubernetes を使用する DevOps チームのニーズに対応しますが、既存の仮想マシン ベースのワークロードには容易にコンテナ化できないものがあります。仮想マシン サービスを使用することで、コンテナ プラットフォームと一緒に Kubernetes 以外のプラットフォームを管理する場合のオーバーヘッドを削減することもできます。Kubernetes プラットフォーム上でコンテナと仮想マシンを実行する場合、DevOps チームはワークロードの占有量を 1 つのプラットフォームに統合できます。

注： 仮想マシン サービスは、スタンドアローン仮想マシンのほか、Tanzu Kubernetes Grid クラスタを構成する仮想マシンも管理します。クラスタの詳細については、『vSphere IaaS 制御プレーンでの TKG サービスの使用』ドキュメントを参照してください。



仮想マシン サービスを使用してデプロイされた各仮想マシンは、vSphere IaaS control plane インフラストラクチャ上で、独自のオペレーティング システムを含むすべてのコンポーネントを実行する完全なマシンとして機能します。仮想マシンは、スーパーバイザー が提供するネットワークおよびストレージにアクセスすることができ、標準の Kubernetes コマンド `kubectl` を使用して管理されます。仮想マシンは完全に隔離されたシステムとして動作し、Kubernetes 環境内の他の仮想マシンまたはワークロードからの干渉を受けません。

Kubernetes プラットフォームで仮想マシンを使用する場合

一般に、コンテナと仮想マシンのどちらでワークロードを実行するかは、ビジネス ニーズおよび目標に応じて決まります。仮想マシンを使用する理由には、次のようなものがあります。

- アプリケーションのコンテナ化ができません。
- アプリケーションが、カスタム カーネルまたはカスタム オペレーティング システム用に設計されています。
- アプリケーションが、仮想マシンで実行するのに適しています。
- 一貫性のある Kubernetes 環境により、オーバーヘッドを回避することを検討しています。Kubernetes 以外のプラットフォームとコンテナ プラットフォームにインフラストラクチャ セットを個別に実行するのではなく、これらのスタックを統合し、使い慣れた `kubectl` コマンドを使用して管理することができます。

スーパーバイザー でのスタンドアローン仮想マシンのデプロイと管理については、『vSphere IaaS 制御プレーンのサービスとワークロード』ドキュメントの仮想マシンのデプロイと管理を参照してください。

vSphere IaaS control plane の スーパーバイザー サービス

スーパーバイザー サービス は、Infrastructure-as-a-Service コンポーネントと緊密に統合された独立系ソフトウェア ベンダー サービスを開発者に提供する vSphere 認定の Kubernetes オペレータです。vSphere IaaS control plane 環境に スーパーバイザー サービス をインストールして管理し、Kubernetes ワークロードで使用可能にすることができます。スーパーバイザー サービス が スーパーバイザー にインストールされている場合、DevOps エンジニアはサービス API を使用して、ユーザー名前空間内の スーパーバイザー にインスタンスを作成できます。これらのインスタンスは、vSphere ポッド および Tanzu Kubernetes Grid クラスタで使用できます。

サポートされているスーパーバイザー サービスの詳細と、サービス YAML ファイルのダウンロード方法については、http://vmware.com/go/supervisor-service を参照してください。

スーパーバイザー サービスの使用方法については、『vSphere IaaS 制御プレーンのサービスとワークロード』ドキュメントの「スーパーバイザー サービスの管理」を参照してください。

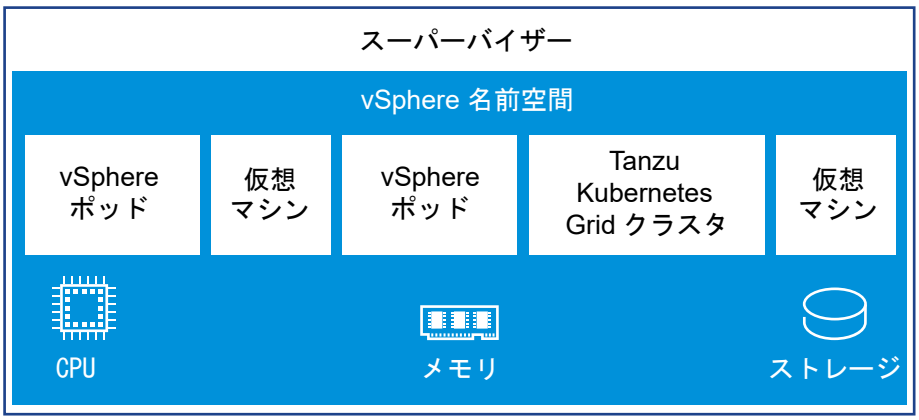
vSphere 名前空間 について

vSphere 名前空間 は、vSphere ポッド、仮想マシン、および Tanzu Kubernetes Grid クラスタを実行できるリソースの境界を設定します。vSphere 管理者は、vSphere Client を使用して vSphere 名前空間 を作成および構成します。

最初に作成された vSphere 名前空間 には、スーパーバイザー 内の無制限のリソースがあります。vSphere 管理者は、CPU、メモリ、ストレージのほか、vSphere 名前空間 内で実行できる Kubernetes オブジェクトの数に制限を設定できます。ストレージ制限は、Kubernetes ではストレージ割り当てと表されます。リソース プールは、スーパーバイザー の vSphere 名前空間 ごとに vSphere 内に作成されます。

vSphere Zones で有効になっている スーパーバイザー では、ゾーンにマッピングされた各 vSphere クラスタに名前空間リソース プールが作成されます。vSphere 名前空間 は、vSphere Zones に含まれている 3 つの vSphere クラスタすべてに分散されます。3 ゾーンの スーパーバイザー の vSphere 名前空間 に使用されるリソースは、基盤となる 3 つのすべての vSphere クラスタから均等に取得されます。たとえば、300 MHz の CPU を使用する場合は、各 vSphere クラスタから 100 MHz が取得されます。

図 1-5. vSphere 名前空間



DevOps エンジニアが名前空間にアクセスできるようにするために、vSphere 管理者は、vCenter Single Sign-On に関連付けられている ID ソース内、または スーパーバイザー に登録された OIDC プロバイダから使用可能なユーザーまたはユーザー グループに権限を割り当てます。詳細については、『vSphere IaaS control plane ID とアクセスの管理』を参照してください。

名前空間が作成され、リソースとオブジェクトの制限、権限、およびストレージ ポリシーが構成されたら、DevOps エンジニアは名前空間にアクセスして、ワークロード（Tanzu Kubernetes Grid クラスタ、vSphere ポッド、仮想マシン サービスを使用して作成された仮想マシンなど）を実行することができます。

vSphere 名前空間 と Kubernetes 名前空間の違い

基本的に、vSphere 名前空間 は Kubernetes 名前空間と同じ機能を提供しますが、vSphere 名前空間 は vSphere IaaS control plane に固有です。vSphere 名前空間 を Kubernetes 名前空間と混同しないでください。

vSphere 名前空間 は、vSphere リソース プールの拡張機能として実装され、スーパーバイザー で実行されているワークロードにリソースを提供します。vSphere 名前空間 では、Kubernetes 名前空間への直接マッピングを使用して、オブジェクトとストレージの割り当てがワークロードに適用されます。

通常の Kubernetes 名前空間とのもう 1 つの違いは、前述のように、vSphere 管理者が vSphere 名前空間 へのユーザー アクセスを管理する点です。vSphere 管理者は、仮想マシン クラスおよび DevOps エンジニアが仮想マシンのセルフサービスに使用できる仮想マシン テンプレートを含むコンテンツ ライブラリを関連付けることもできます。詳細については、vSphere IaaS 制御プレーンのサービスとワークロードでの仮想マシンのデプロイと管理を参照してください。

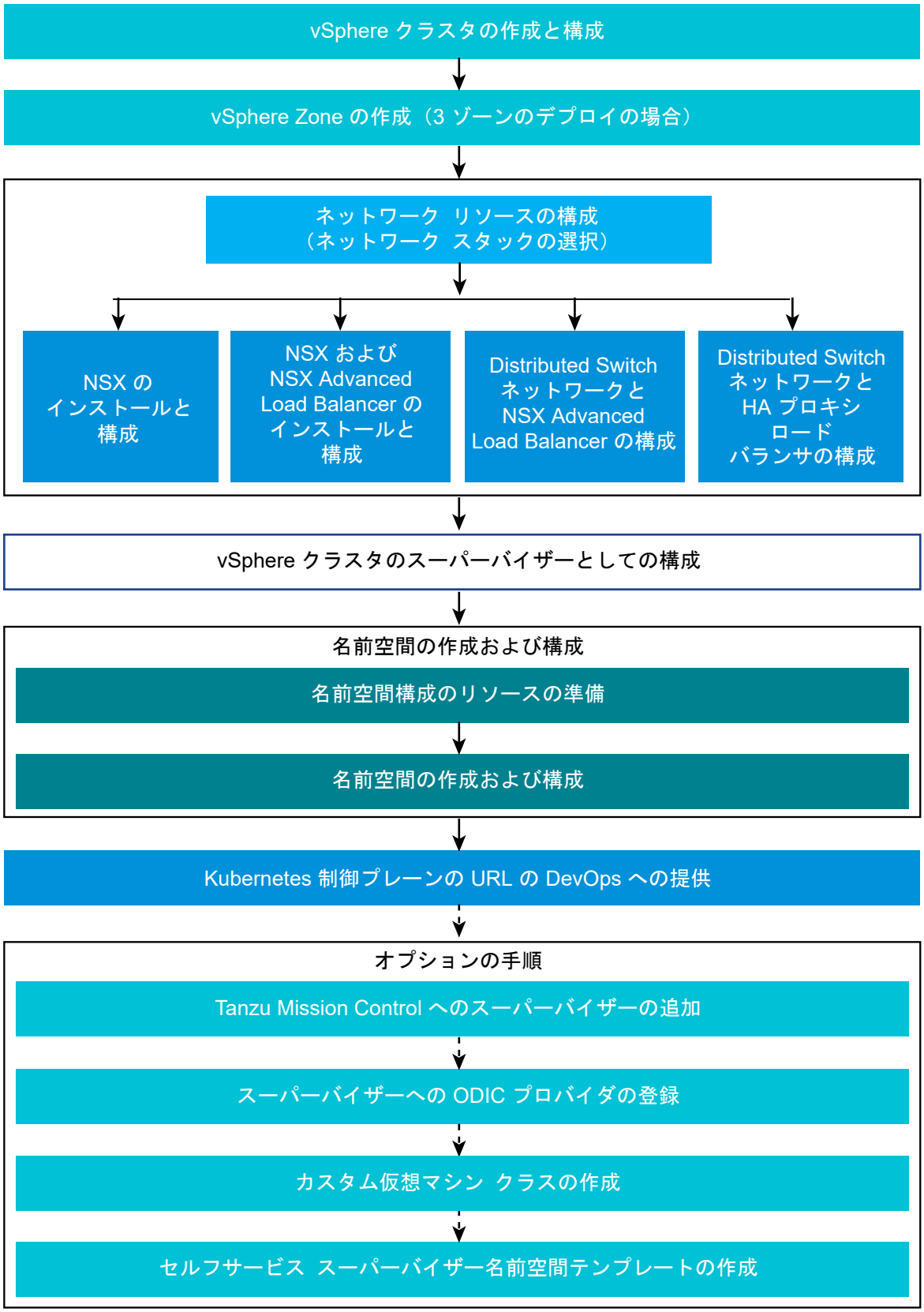
vSphere IaaS control plane のユーザー ロールとワークフロー

vSphere IaaS control plane には、vSphere 管理者と DevOps エンジニアの 2 つのロールがあります。DevOps エンジニアは、DevOps、アプリケーション開発者、および Kubernetes 管理者のロールで構成されます。これらのロールは、それぞれ異なるインターフェイスを通じてプラットフォームと通信します。vCenter Server でこれらのロールのユーザーまたはユーザー グループを定義し、権限を関連付けることができます。vSphere 管理者ロールと DevOps エンジニア ロールのワークフローは異なり、これらのロールで必要となる専門知識の特定の領域によって決定されます。

ユーザー ロールとワークフロー

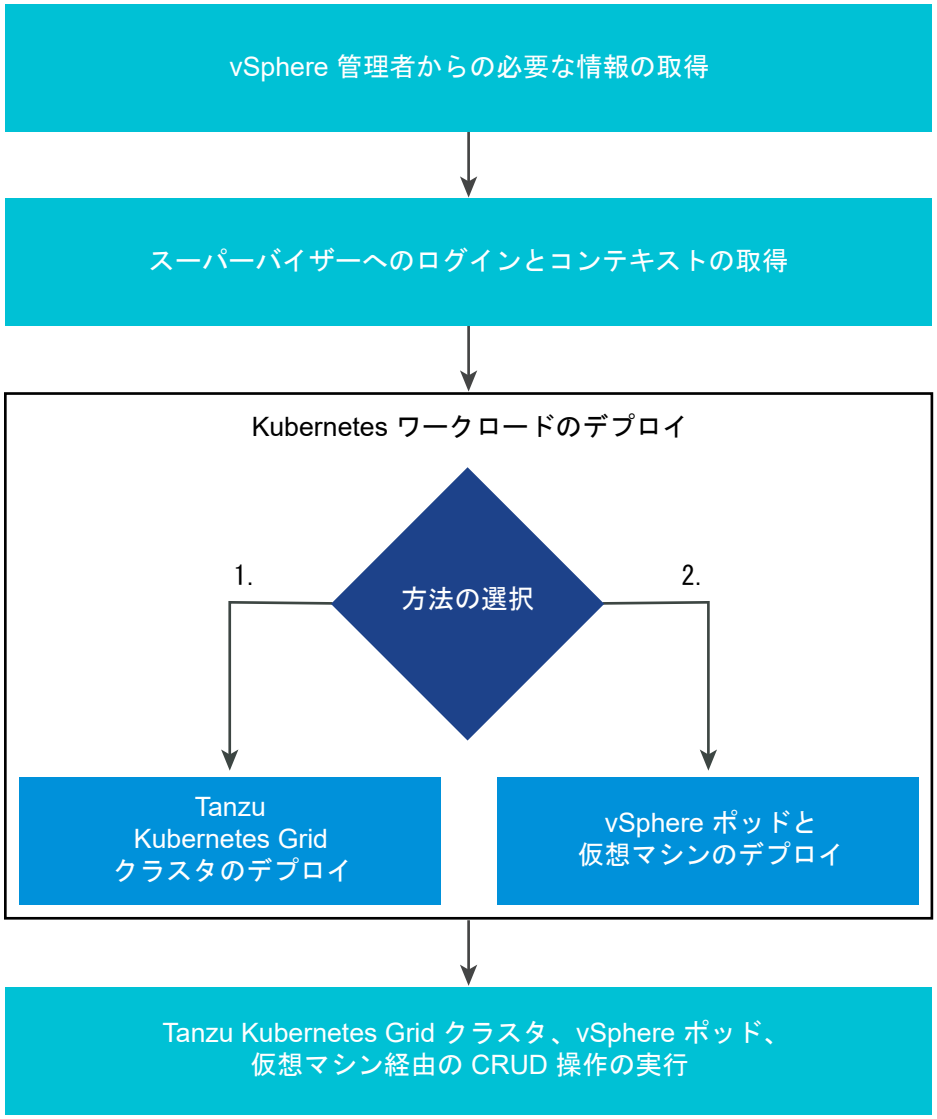
vSphere 管理者が vSphere IaaS control plane と通信するための主要インターフェイスは vSphere Client です。大まかに、vSphere 管理者の責務には、DevOps エンジニアが Kubernetes ワークロードをデプロイできるように スーパーバイザー と名前空間を構成することが含まれます。vSphere、NSX Advanced Load Balancer または HAProxy ロード バランサ、NSX（このネットワーク スタックを選択した場合）について優れた知識を持ち、Kubernetes の基本を理解している必要があります。

図 1-6. vSphere 管理者の大まかなワークフロー



DevOps エンジニアには、Kubernetes 開発者およびアプリケーション所有者と、Kubernetes 管理者、またはその両方を組み合わせた役割があります。DevOps エンジニアは、kubectl コマンドを使用して、既存の名前空間に vSphere ポッド と仮想マシンをデプロイします。また、kubectl と Tanzu CLI を使用して、Tanzu Kubernetes Grid クラスタのデプロイと管理を行います。通常、DevOps エンジニアは vSphere、NSX、Distributed Switch、NSX Advanced Load Balancer、HAProxy のエキスパートである必要はありませんが、これらのテクノロジーとプラットフォームに関する基礎知識があれば、vSphere 管理者とより効率的にやり取りすることができます。

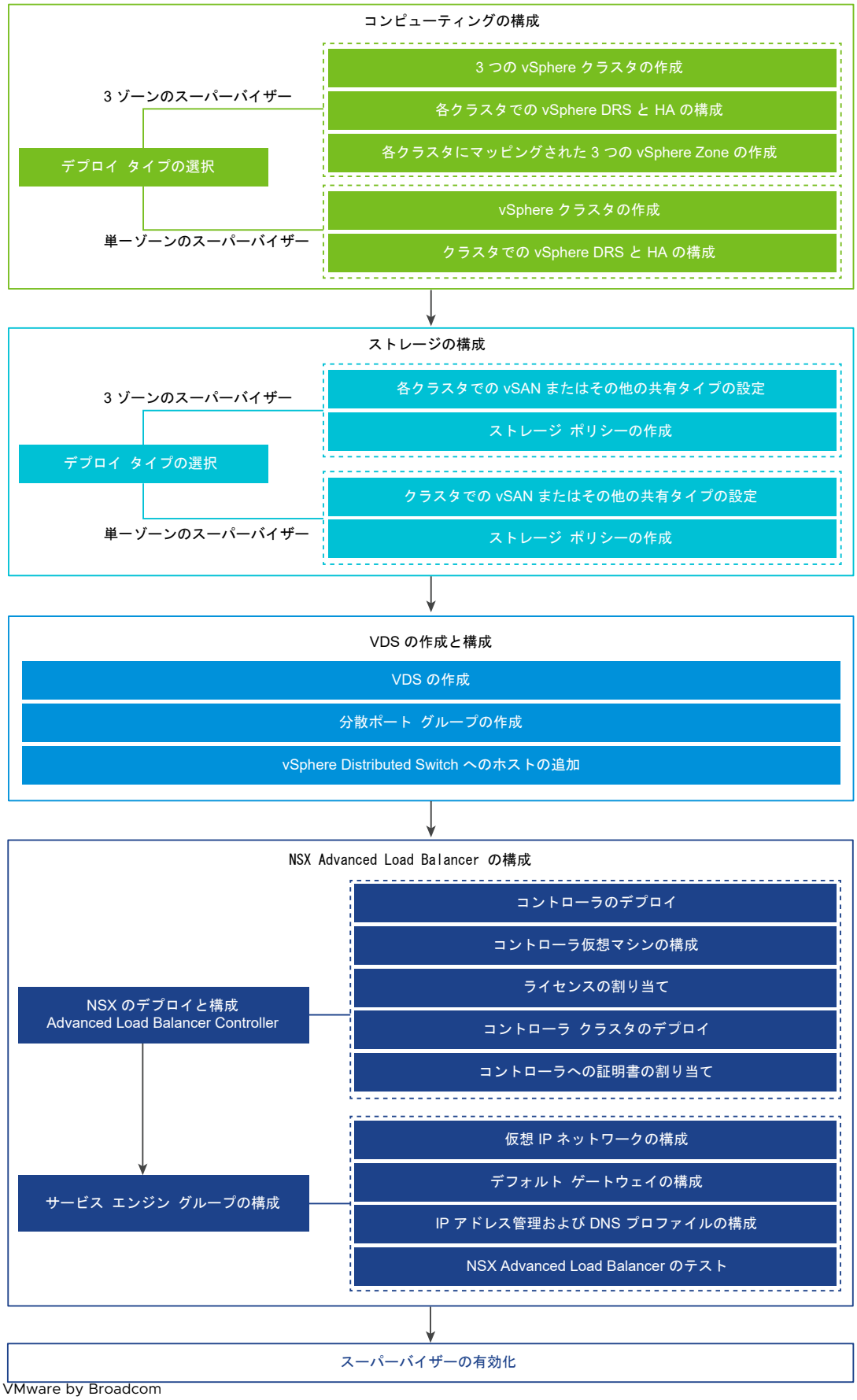
図 1-7. DevOps エンジニアの大まかなワークフロー



Distributed Switch ネットワークと NSX Advanced Load Balancer を使用する スーパーバイザー のワークフロー

vSphere 管理者は、vSphere クラスタを、Distributed Switch と NSX Advanced Load Balancer を介した vSphere ネットワーク スタックを使用する スーパーバイザー として構成できます。1 つの vSphere クラスタにマッピングされた 1 ゾーンの スーパーバイザー、または 3 つの vSphere クラスタにマッピングされた 3 ゾーンの スーパーバイザー を構成できます。システム要件の詳細については、スーパーバイザー および Distributed Switch ネットワークを使用したクラスタ NSX Advanced Load Balancer デプロイの要件および NSX Advanced Load Balancer および Distributed Switch ネットワークを使用したゾーン スーパーバイザー デプロイの要件を参照してください。Distributed Switch ネットワークでスーパーバイザーを有効にする方法については、『vSphere IaaS 制御プレーンのインストールと構成』の「インストールと構成」を参照してください。

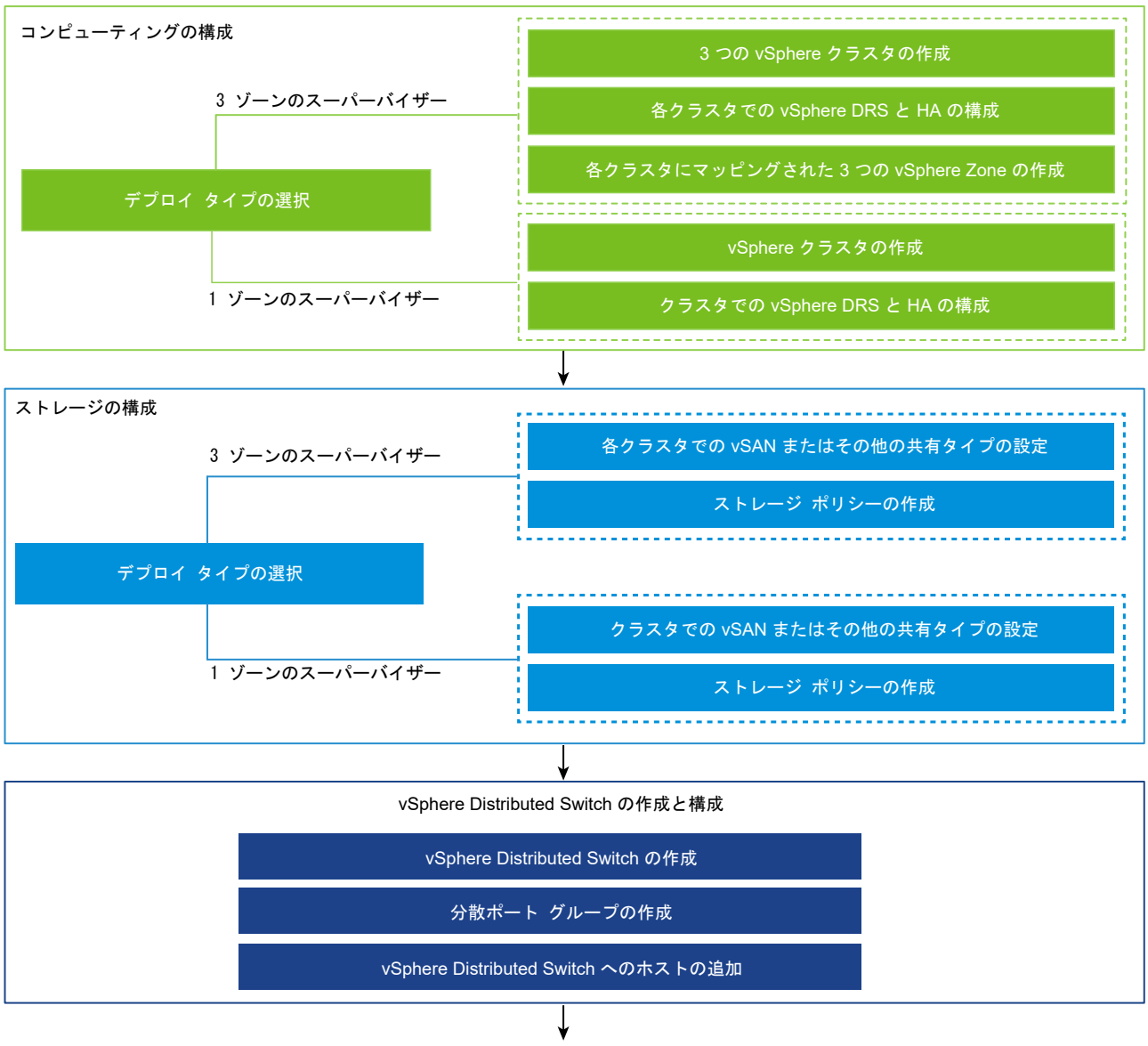
図 1-8. Distributed Switch ネットワークと NSX Advanced Load Balancer を使用した スーパーバイザーの有効化のワークフロー

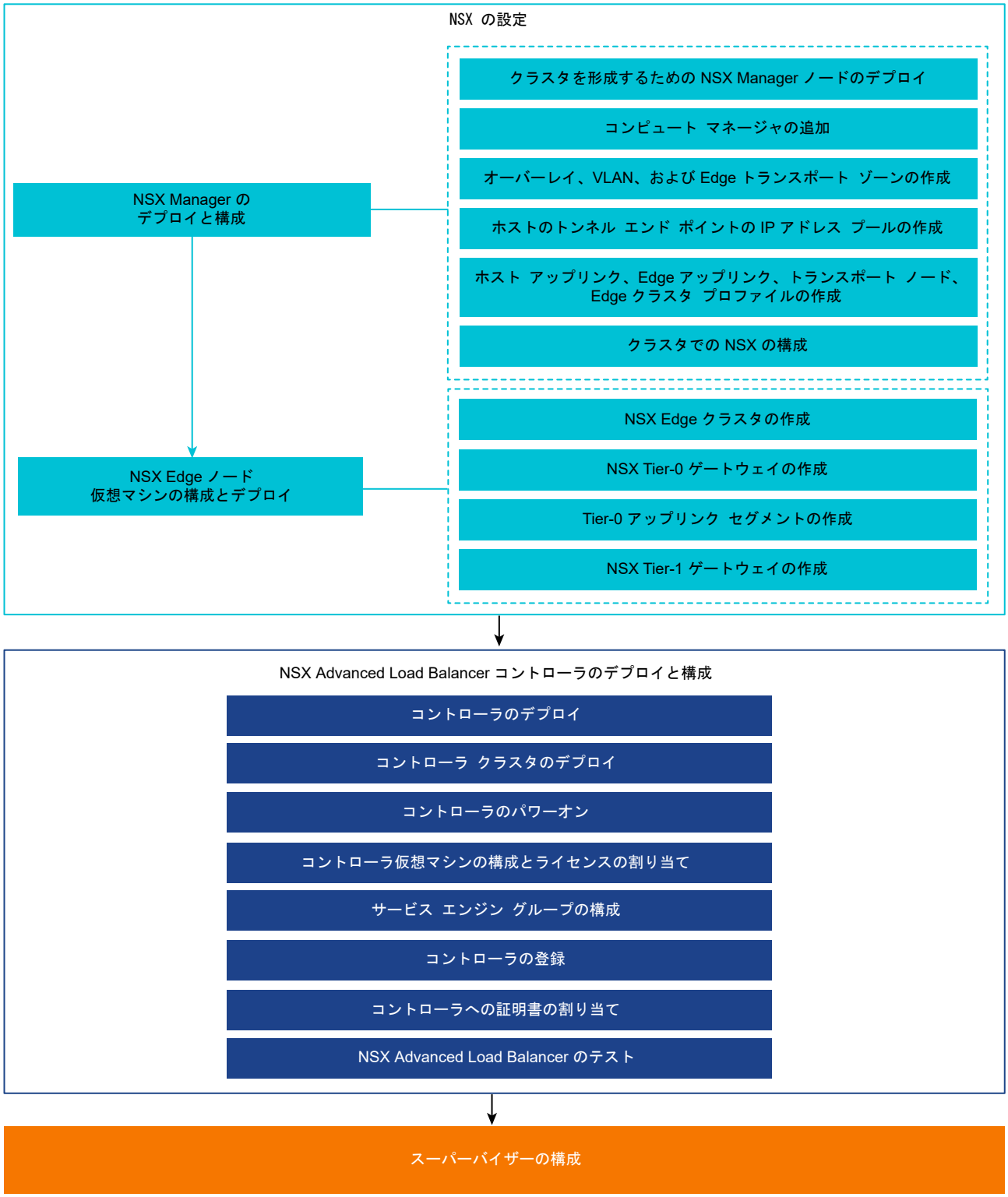


NSX ネットワークと NSX Advanced Load Balancer Controller を使用する スーパーバイザー のワークフロー

NSX ネットワーク スタックと NSX Advanced Load Balancer Controller を使用して、1 ゾーンまたは 3 ゾーンの スーパーバイザー を構成できます。要件の詳細については、「NSX および NSX Advanced Load Balancer を使用したクラスタ スーパーバイザー のデプロイの要件」および「NSX および NSX Advanced Load Balancer でのゾーン スーパーバイザー の要件」を参照してください。インストール手順については、「NSX および NSX Advanced Load Balancer のインストールと構成」を参照してください。

図 1-9. NSX ネットワークと NSX Advanced Load Balancer Controller を使用してスーパーバイザーを有効にするためのワークフロー

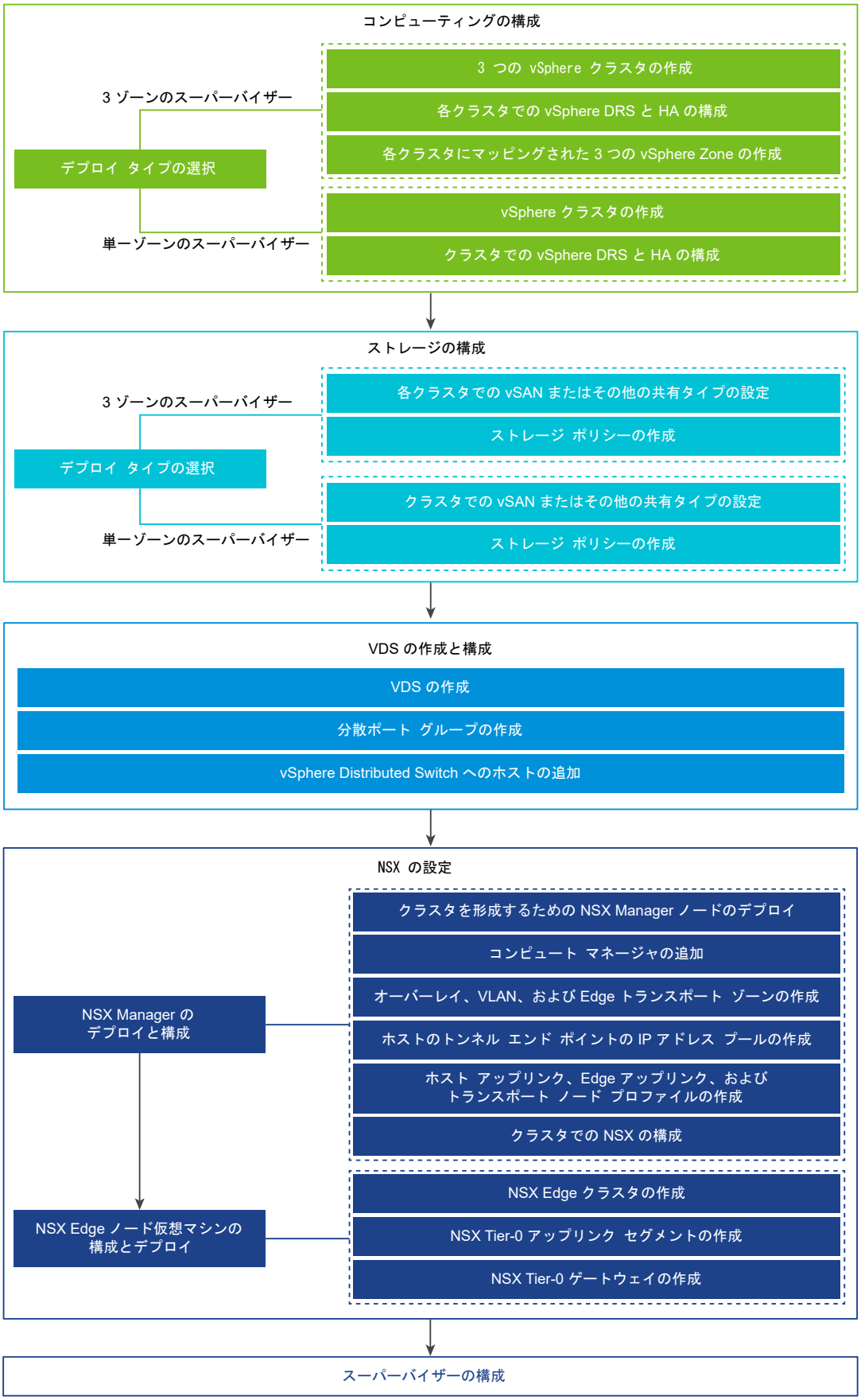



NSX の設定
クラスタを形成するための NSX Manager ノードのデプロイ
コンピュート マネージャの追加
オーバーレイ、VLAN、および Edge トランスポート ゾーンの作成
ホストのトンネル エンド ポイントの IP アドレス プールの作成
ホスト アップリンク、Edge アップリンク、トランスポート ノード、Edge クラスタ プロファイルの作成
クラスタでの NSX の構成
NSX Manager のデプロイと構成
NSX Edge ノード仮想マシンの構成とデプロイ
NSX Edge クラスタの作成
NSX Tier-0 ゲートウェイの作成
Tier-0 アップリンク セグメントの作成
NSX Tier-1 ゲートウェイの作成
NSX Advanced Load Balancer コントローラのデプロイと構成
コントローラのデプロイ
コントローラ クラスタのデプロイ
コントローラのパワーオン
コントローラ仮想マシンの構成とライセンスの割り当て
サービス エンジン グループの構成
コントローラの登録
コントローラへの証明書の割り当て
NSX Advanced Load Balancer のテスト
スーパーバイザーの構成

NSX ネットワークを使用する スーパーバイザー のワークフロー

NSX をネットワーク スタックとして使用して、1 ゾーンまたは 3 ゾーンの スーパーバイザー を構成することもできます。システム要件の詳細については、NSX を使用したクラスタ スーパーバイザー のデプロイの要件および NSX でのゾーン スーパーバイザー の要件を参照してください。インストール手順については、『vSphere IaaS 制御プレーンのインストールと構成』の「インストールと構成」を参照してください。

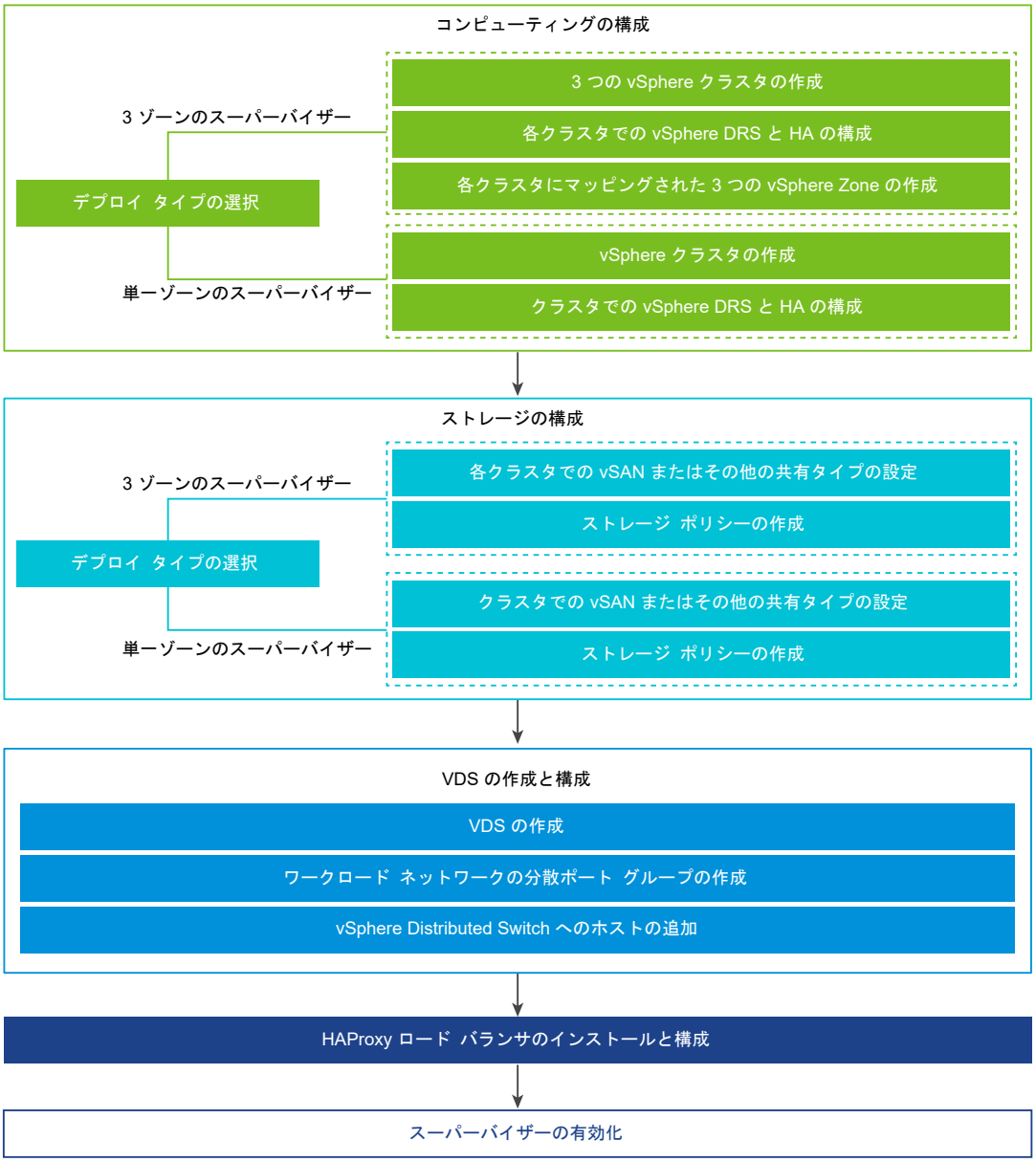
図 1-10. NSX ネットワークを使用したスーパーバイザーの有効化のワークフロー



Distributed Switch ネットワークと HAProxy ロード バランサを使用する スーパーバイザー のワークフロー

vSphere 管理者は、Distributed Switch ネットワーク スタックと HAProxy ロード バランサを使用して、vSphere クラスタにマッピングされた 1 つまたは 3 つの vSphere Zone で スーパーバイザー を有効にすることができます。システム要件の詳細については、Distributed Switch ネットワークと HAProxy ロード バランサを使用したクラスタ スーパーバイザー のデプロイの要件および HA プロキシ ロード バランサを使用したゾーン スーパーバイザー デプロイの要件を参照してください。インストール手順については、『vSphere IaaS 制御プレーンのインストールと構成』の「インストールと構成」を参照してください。

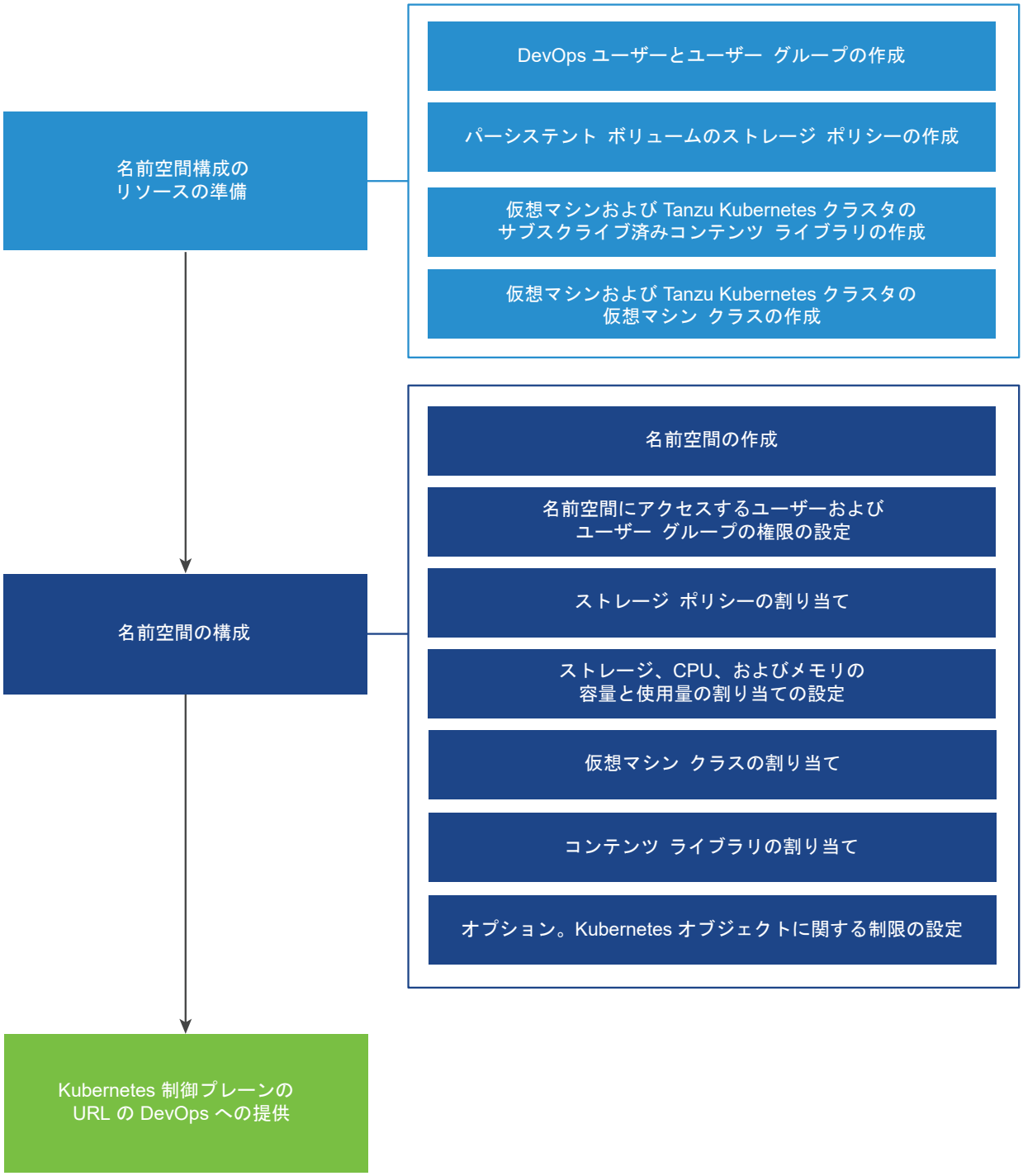
図 1-11. Distributed Switch ネットワークと HAProxy を使用したスーパーバイザーの有効化のワークフロー



名前空間の作成と構成のワークフロー

スーパーバイザー を有効にしたら、vSphere 管理者は、スーパーバイザー で vSphere 名前空間 を作成して構成します。実行するアプリケーションとワークロードについて DevOps エンジニアから特定のリソース要件を収集し、それに応じて名前空間を構成する必要があります。詳細については vSphere 名前空間の構成と管理を参照してください。

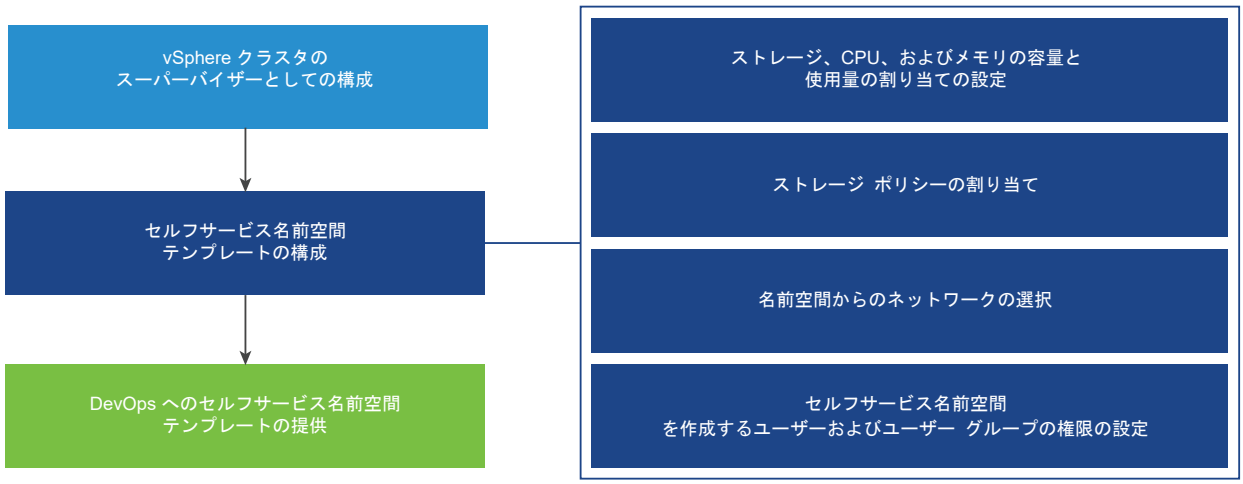
図 1-12. vSphere 名前空間の構成のワークフロー



セルフサービス名前空間の作成と構成のワークフロー

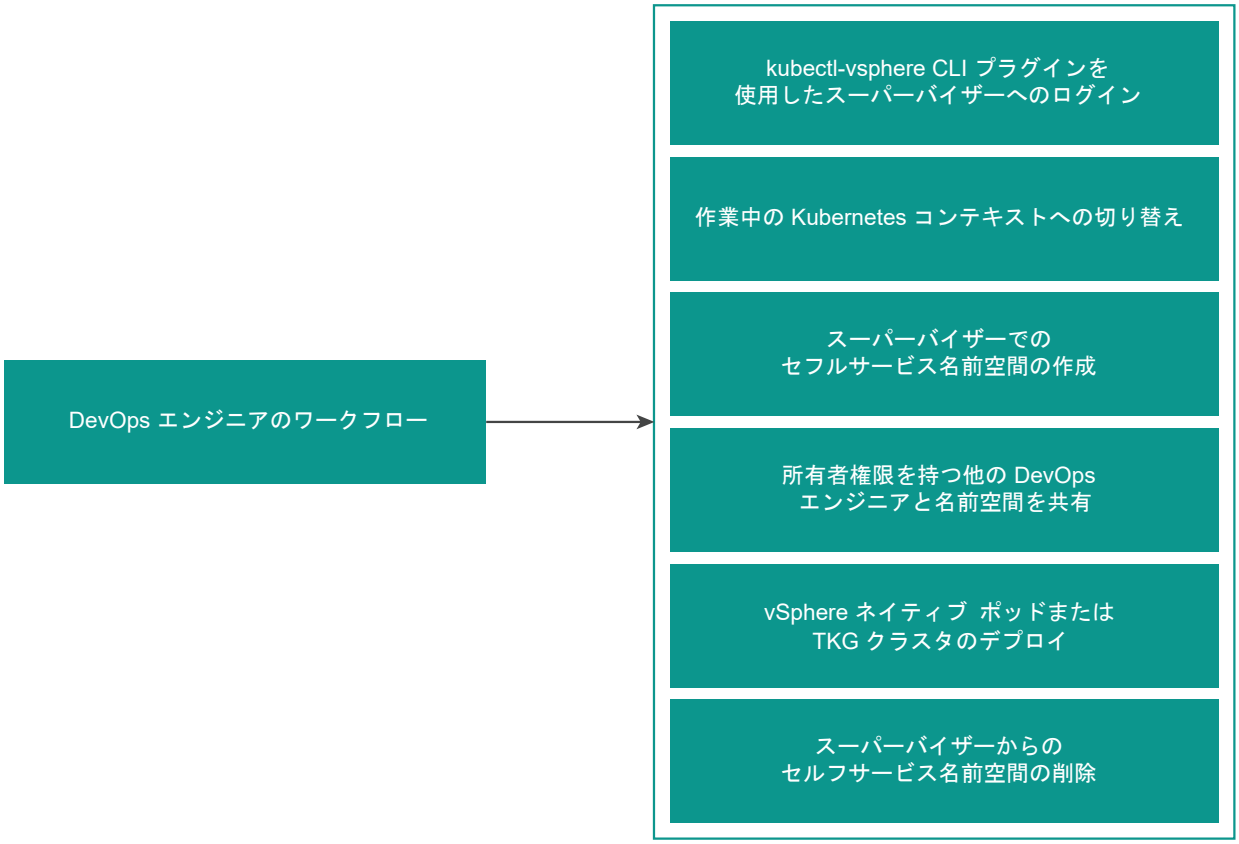
vSphere 管理者は、vSphere 名前空間 の作成、名前空間に対する CPU、メモリ、ストレージの制限の設定、権限の割り当て、およびクラスタの名前空間サービスのテンプレートとしてのプロビジョニングと有効化を行うことができます。詳細については vSphere 名前空間の構成と管理を参照してください。

図 1-13. セルフサービス名前空間テンプレートのプロビジョニングのワークフロー



DevOps エンジニアは、セルフ サービス方式で vSphere 名前空間 を作成し、その中にワークロードをデプロイすることができます。また、他の DevOps エンジニアと名前空間を共有したり、不要になった名前空間を削除したりできます。

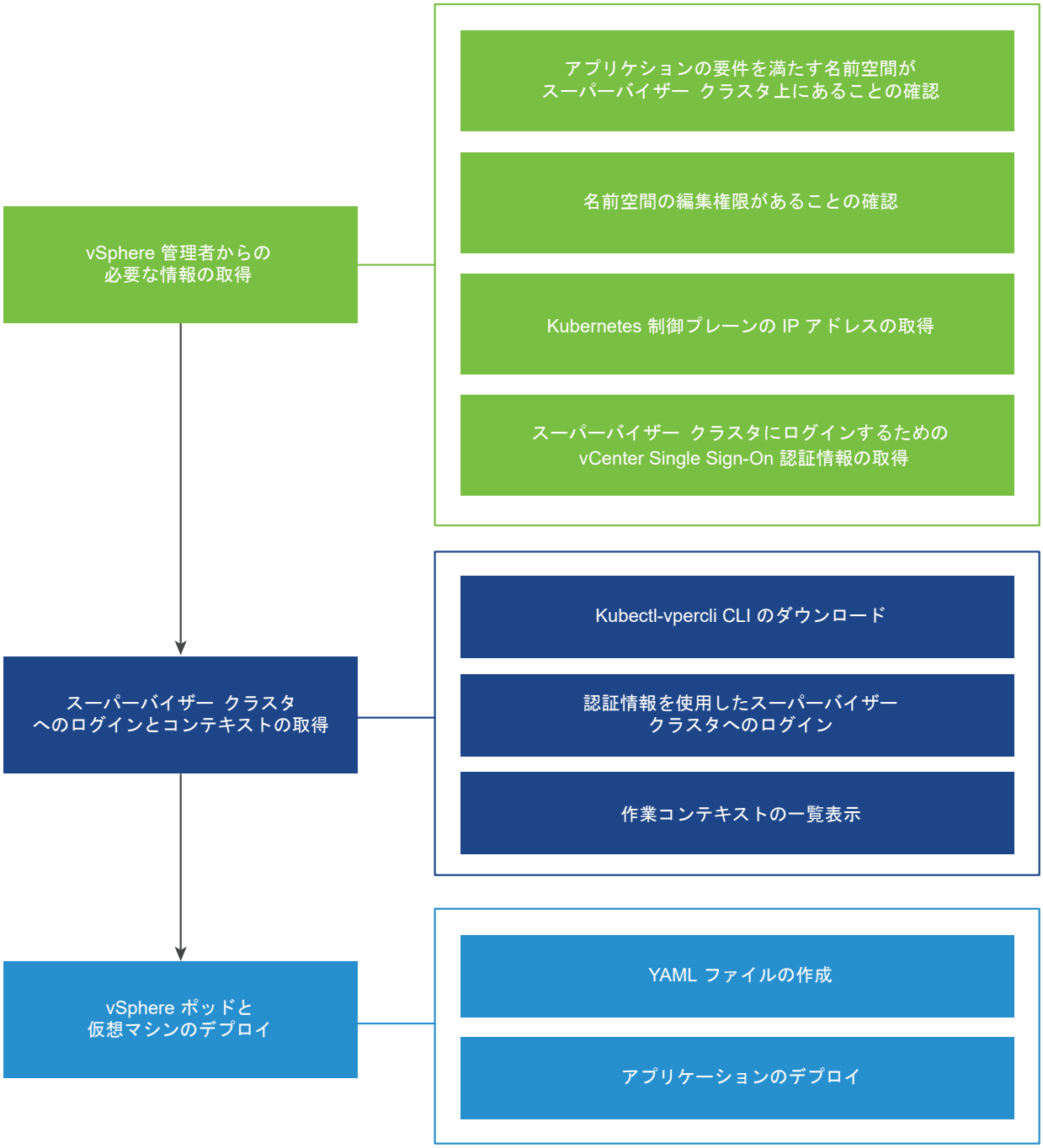
図 1-14. セルフサービス名前空間の作成のワークフロー



vSphere ポッド と仮想マシンのプロビジョニング ワークフロー

DevOps エンジニアは、スーパーバイザー で実行されている名前空間のリソースの境界内で vSphere ポッド および仮想マシンをデプロイできます。詳細については、『vSphere IaaS 制御プレーンのサービスとワークロード』の「vSphere ポッドへのワークロードのデプロイ」および「仮想マシンのデプロイと管理」を参照してください。

図 1-15. vSphere ポッド と仮想マシンのプロビジョニング ワークフロー



Tanzu Kubernetes Grid クラスタのプロビジョニング ワークフロー

DevOps エンジニアは、vSphere 名前空間 に Tanzu Kubernetes Grid クラスタを作成および構成します。詳細については、『vSphere IaaS 制御プレーンでの TKG サービスの使用』ガイドを参照してください。

vSphere IaaS control plane による vSphere 環境の変革

スーパーバイザー では、名前空間、vSphere ポッド、Tanzu Kubernetes Grid クラスタなどのオブジェクトが vCenter Server インベントリに追加されます。

各 スーパーバイザー で、次のものを表示できます。

- クラスタで実行されている論理アプリケーションを表す名前空間。
- スーパーバイザー の各名前空間のリソース プール。3 ゾーン デプロイでは、名前空間ごとのリソース プールがゾーンの各クラスタ部分で作成されます。

すべての名前空間内で、次のものを表示できます。

- vSphere ポッド。
- Tanzu Kubernetes Grid クラスタ。
- Kubernetes 制御プレーン仮想マシンとスタンドアローン仮想マシン。
- ネットワークおよびストレージ リソース。
- その名前空間のユーザー権限。

vSphere IaaS control plane のライセンス

スーパーバイザー に割り当てることができる各種ライセンスのほか、ライセンス コンプライアンス、評価期間、ライセンスの有効期限の仕組みについて説明します。

スーパーバイザー のライセンス

vSphere クラスタで スーパーバイザー を有効にすると、60 日の評価期間の間、スーパーバイザー のすべての機能を使用できるようになります。60 日の評価期間が終了する前に、有効なライセンスを スーパーバイザー に割り当てる必要があります。

VCF および VVF ソリューション ライセンス

vSphere 8 Update 2b リリース以降では、vSphere IaaS control plane の VMware vSphere Foundation (VVF) または VMware Cloud Foundation (VCF) ソリューション ライセンスを使用できます。vCenter Server をバージョン 8 Update 2b にアップグレードすると、VVF または VCF ソリューション ライセンスを vSphere 環境内の スーパーバイザー に割り当てることができます。

注： 個々のコンポーネントのライセンス キーは引き続きサポートされます。それらはソリューション ライセンスとともに提供されます。環境内では、ソリューション ライセンス、個々のコンポーネントのライセンス、またはその両方を使用できます。

Tanzu エディション ライセンス

vSphere 8 Update 2b を実行していて、スーパーバイザー に有効な Tanzu エディション ライセンスがすでに付与されている場合、そのライセンスは期限切れになるまで引き続き有効です。Tanzu ライセンスの有効期限が切れたら、VCF または VVF ソリューション ライセンスを スーパーバイザー または有効な Tanzu ライセンスに割り当てる必要があります。

ライセンスの有効期限

ソリューション ライセンスまたは Tanzu エディション ライセンスの有効期限が切れても、新しいライセンスを入手するまで vSphere IaaS control plane のすべての機能を引き続き使用できます。ただし、期限切れのライセンスを新しい スーパーバイザー に割り当てることはできません。

評価期間の有効期限

スーパーバイザー の評価期間が終了した場合、vSphere 管理者は新しい vSphere 名前空間 を作成することも、スーパーバイザー の Kubernetes バージョンをアップデートすることもできません。DevOps エンジニアが新しいワークロードをデプロイすることはできません。また、新しいノードの追加など、既存の Tanzu Kubernetes Grid クラスタの構成を変更することもできません。

引き続き Tanzu Kubernetes Grid クラスタにワークロードをデプロイして、既存のすべてのワークロードに予期した動作を継続させることはできます。すでにデプロイされているすべての Kubernetes ワークロードは、通常の動作を継続します。

ライセンス コンプライアンス

ソリューション ライセンスまたは Tanzu ライセンス キーには、ESXi ホスト ライセンスと同様に、CPU あたり最大 32 コアの CPU キャパシティがあります。これらのライセンスのいずれかを スーパーバイザー に割り当てる場合、使用されるキャパシティの量は、クラスタ内のホスト上の CPU の数と各 CPU のコア数によって決まります。ソリューション ライセンスまたは Tanzu エディション ライセンス キーは一度に複数の スーパーバイザー に割り当てることができますが、複数のライセンス キーを 1 つの スーパーバイザー に割り当てることはできません。

たとえば、新しいホストを追加して スーパーバイザー を拡張し、スーパーバイザー に割り当てられたライセンス キーがキャパシティ不足になった場合、同じライセンス キーを引き続き使用できます。ただし、EULA への準拠を維持するには、スーパーバイザー のすべての CPU とコアに十分対応できるキャパシティのある新しいライセンス キーを取得する必要があります。

vSphere IaaS control plane のライセンス

提供されるライセンスは、vSphere IaaS control plane の構成に使用したネットワーク スタックによって異なります。

スーパーバイザー の設定	vSphere 8 Update 2b のライセンス	vSphere 8 Update 2b より前のライセンス
VDS ネットワークと NSX Advanced Load Balancer を使用する スーパーバイザー	■ VCF ソリューション ライセンス ■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス ■ NSX Advanced Load Balancer Essentials	■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス ■ NSX Advanced Load Balancer Essentials
VDS ネットワークと HAProxy ロード バランサを使用する スーパーバイザー	■ VVF ソリューション ライセンス ■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス	■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス
スーパーバイザー と NSX	■ VVF ソリューション ライセンス ■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス ■ NSX Advanced 以降	■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス ■ NSX Advanced 以降
NSX と NSX Advanced Load Balancer を使用する スーパーバイザー	■ VCF ソリューション ライセンス ■ NSX Advanced Load Balancer Enterprise ■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス ■ NSX Advanced 以降 ■ NSX Advanced Load Balancer Enterprise	■ vSphere Enterprise+ ライセンス ■ Tanzu エディション ライセンス ■ NSX Advanced 以降 ■ NSX Advanced Load Balancer Enterprise

vSphere IaaS control plane ID とアクセスの管理

vSphere 管理者には、スーパーバイザー を有効にして構成する権限、および vSphere 名前空間 を管理する権限が必要です。名前空間の権限を定義して、どの DevOps エンジニアと開発者が名前空間にアクセスできるかを決定します。また、外部 OpenID Connect (OIDC) プロバイダを使用して スーパーバイザー を構成し、多要素認証を有効にすることもできます。DevOps エンジニアまたは開発者は、vSphere 管理者が スーパーバイザー で構成した内容に応じて、vCenter Single Sign-On の認証情報または OIDC プロバイダからの認証情報を使用して スーパーバイザー で認証します。権限を持つ vSphere 名前空間 にのみアクセスできます。

サポートされている ID プロバイダ

vSphere IaaS control plane は、次の ID プロバイダをサポートしています。

- vCenter Single Sign-On。スーパーバイザー と Tanzu Kubernetes Grid クラスタを含む、vSphere IaaS control plane 環境での認証に使用するデフォルトの ID プロバイダです。vCenter Single Sign-On は、vSphere インフラストラクチャに認証を提供し、AD/LDAP システムと統合できます。vCenter Single Sign-On の詳細については、vCenter Single Sign-On による vSphere 認証を参照してください。
- 外部 ID プロバイダ。vSphere 管理者は、OpenID Connect プロトコルをサポートする外部 ID プロバイダを使用して スーパーバイザー を構成できます。外部 ID プロバイダが構成されている スーパーバイザー は

OAuth 2.0 クライアントとして機能し、Pinniped 認証サービスを使用して、Tanzu CLI 経由で Tanzu Kubernetes Grid クラスタに接続します。Tanzu CLI は、Tanzu Kubernetes Grid クラスタのライフサイクルのプロビジョニングと管理をサポートします。各 スーパーバイザー インスタンスは、外部 ID プロバイダを 1 つのみサポートします。

スーパーバイザー での認証

vSphere IaaS control plane を操作するさまざまなロールは、次の方法を使用して スーパーバイザー で認証できます。

- vSphere 管理者。vSphere 管理者は、vCenter Single Sign-On を使用して、vSphere Client を介して vSphere で認証します。kubectl 向けの vSphere プラグイン を使用して、kubectl を介して スーパーバイザー と Tanzu Kubernetes Grid クラスタで認証することもできます。詳細については、「vCenter Single Sign-On ユーザーとしてスーパーバイザーに接続する」を参照してください。
- DevOps エンジニアまたは開発者。DevOps エンジニアまたは開発者は、vCenter Single Sign-On を使用して、kubectl 向けの vSphere プラグイン と kubectl を介して スーパーバイザー で認証します。スーパーバイザー が構成されている外部 ID プロバイダの認証情報を使用して、スーパーバイザー に接続することもできます。詳細については、「外部 ID プロバイダを使用したスーパーバイザー上の TKG クラスタへの接続」を参照してください。

スーパーバイザー を使用したログイン セッション

スーパーバイザー に vCenter Single Sign-On ユーザーとしてログインすると、認証プロキシによって要求が vCenter Single Sign-On にリダイレクトされます。kubectl 向けの vSphere プラグイン は、vCenter Server とのセッションを確立し、vCenter Single Sign-On から認証トークンを取得します。また、アクセスできる vSphere 名前空間 のリストを取得し、これらの vSphere 名前空間 を構成にポピュレートします。ユーザー アカウントの権限に変更があった場合は、次回ログイン時に vSphere 名前空間 のリストが更新されます。

スーパーバイザー にログインする際に使用するアカウントでアクセスできるのは、自分に割り当てられている vSphere 名前空間 のみです。vCenter Server にログインするには、vSphere 管理者が 1 つ以上の vSphere 名前空間 でアカウントに適切な権限を設定する必要があります。

注： kubectl へのセッションは 10 時間継続します。セッションの期限が切れると、スーパーバイザー で再度認証する必要があります。ログアウト時にトークンはユーザー アカウントの構成ファイルから削除されますが、セッションが終了するまで有効なままです。

Tanzu Kubernetes Grid クラスタを使用した認証

DevOps エンジニアまたは開発者は、プロビジョニングされた Tanzu Kubernetes Grid クラスタに接続して、それらを運用および管理します。Tanzu Kubernetes Grid クラスタがプロビジョニングされている vSphere 名前空間 に対する編集権限または所有者権限がユーザー アカウントに付与されると、そのアカウントが `cluster-admin` ロールに割り当てられます。または、`kubernetes-admin` ユーザーを使用して、Tanzu Kubernetes Grid に接続することもできます。ユーザーまたはグループをデフォルトまたはカスタムのポッド セキュリティ ポリシーにバインドすることにより、開発者に Tanzu Kubernetes Grid クラスタへのアクセス権を付与することもできます。詳細については、「vCenter SSO 認証を使用したスーパーバイザー上の TKG クラスタへの接続」および「外部 ID プロバイダを使用したスーパーバイザー上の TKG クラスタへの接続」を参照してください。

vSphere 名前空間 ロールの権限

vSphere 管理者は、vSphere 名前空間 で DevOps エンジニアまたは開発者に表示、編集、所有者権限を付与します。ユーザーまたはグループは、vCenter Single Sign-On または スーパーバイザー が構成されている外部 ID プロバイダで使用できる必要があります。1 つのユーザーまたはグループで複数の vSphere 名前空間 にアクセスできます。各 vSphere 名前空間 ロールには、次のアクションが許可されます。

ロール	説明
表示可能	ユーザーまたはグループの読み取り専用アクセス。ユーザーまたはグループは、スーパーバイザー 制御プレーンにログインして、vSphere 名前空間 で実行されているワークロード（vSphere ポッド、Tanzu Kubernetes Grid クラスタ、仮想マシンなど）を一覧表示できます。
編集可能	ユーザーまたはグループは、vSphere ポッド、Tanzu Kubernetes Grid クラスタ、仮想マシンを作成、読み取り、更新、および削除できます。管理者グループに属するユーザーには、スーパーバイザー内のすべての名前空間に対する編集権限があります。
所有者	所有者権限を持つユーザーまたはグループは、次の操作を実行できます。 ■ vSphere 名前空間 でワークロードをデプロイおよび管理する。 ■ vSphere 名前空間 を他のユーザーまたはグループと共有する。 ■ kubectl を使用して追加の vSphere 名前空間 を作成および削除する。所有者権限を持つユーザーは名前空間を共有する場合、表示、編集、または所有者権限を他のユーザーまたはグループに割り当てることができます。 **注：** 所有者ロールは、vCenter Single Sign-On で使用可能なユーザーに対してサポートされます。外部 ID プロバイダからのユーザーまたはグループで所有者ロールを使用することはできません。

vSphere 名前空間 の作成と構成の詳細については、「vSphere 名前空間の作成と構成」を参照してください。

vSphere 管理者は、ロールの権限、リソースの割り当て、およびストレージを使用して vSphere 名前空間 を構成したら、スーパーバイザー 制御プレーンの URL を DevOps エンジニアまたは開発者に提供します。DevOps エンジニアまたは開発者はその URL を使用して制御プレーンにログインできます。ログインすると、DevOps エンジニアまたは開発者は、vCenter Server システムに属する、同じ ID プロバイダで構成されている スーパーバイザーで、権限を持つ vSphere 名前空間 にアクセスできます。vCenter Server システムが拡張リンク モードになっている場合、DevOps エンジニアまたは開発者は、リンク モード グループで使用可能なすべての スーパーバイザー内の、権限を持つすべての vSphere 名前空間 にアクセスできます。スーパーバイザー 制御プレーンの IP アドレスは、NSX またはロード バランサ（Distributed Switch ネットワークの場合）によって生成される仮想 IP アドレスで、スーパーバイザー 制御プレーンへのアクセス ポイントとして機能します。

vSphere 管理者の権限

通常、vSphere 管理者はユーザー アカウントに次の権限を付与できます。

オブジェクト	権限
vCenter Single Sign-On ユーザー	管理者グループ
vSphere 名前空間 ユーザー	管理者グループのメンバーには、すべての vSphere 名前空間 に対する編集権限が付与されます。

vSphere IaaS control plane の操作に使用するインターフェイスに応じて、付与された権限に基づくさまざまな操作を実行できます。

インターフェイス	操作
vSphere Client	vSphere Client に管理者としてログインすると、次の操作を実行できます。 ■ スーパーバイザー を有効にして構成する。 ■ DevOps エンジニアまたは開発者のリソースの割り当てとロールの権限を使用して、vSphere 名前空間 を作成および構成する。vSphere 名前空間 のロールの権限は、kubectl を使用して スーパーバイザー 制御プレーンにログインしてワークロードの管理を実行するユーザーまたはグループに必要です。 ■ スーパーバイザー 上の スーパーバイザー サービス をデプロイおよび管理する。
kubectl	vCenter Single Sign-On 管理者アカウントを使用して スーパーバイザー 制御プレーンにログインすると、次の操作を実行できます。 ■ システムの vSphere 名前空間（kube-system およびすべての vmware-system-* 名前空間）を含むすべての vSphere 名前空間 内のリソースを表示する。 ■ システム以外のすべての vSphere 名前空間（vSphere Client または vCenter Server API を使用して作成された名前空間）内のリソースを編集する。 ただし、管理者グループのアカウント部分を使用して スーパーバイザー 制御プレーンにログインした場合、クラスタレベルのリソースの編集、kubectl を使用した vSphere 名前空間 の作成、ロール バインドの作成は許可されません。リソース割り当ての設定、vSphere 名前空間 の作成と構成、ユーザー権限の設定を行うには、vSphere Client をプライマリ インターフェイスとして使用する必要があります。

DevOps エンジニアと開発者の権限

通常、DevOps エンジニアまたは開発者のユーザー アカウントには次の権限が必要です。

オブジェクト	権限
vSphere 名前空間	編集または所有者
vCenter Single Sign-On ユーザー	なし、または読み取り専用

DevOps エンジニアまたは開発者は、vSphere IaaS control plane を操作するためのプライマリ インターフェイスとして kubectl を使用します。自身に割り当てられている vSphere 名前空間 でワークロードを表示、実行、および管理するには、kubectl 向けの vSphere プラグイン を使用して スーパーバイザー 制御プレーンにログインできる必要があります。そのため、ユーザー アカウントには、1 つ以上の vSphere 名前空間 に対する編集または所有者の権限が必要です。

通常、スーパーバイザー に対して管理操作を実行する場合、vSphere Client を使用する必要はありません。ただし、場合によっては、vSphere Client にログインして、アカウントに割り当てられている vSphere 名前空間 内のリソースとワークロードを表示することができます。このために、vSphere に対する読み取り専用権限が必要になる場合があります。

vSphere 名前空間 の権限

vSphere 名前空間の権限は、vSphere IaaS control plane の操作方法を制御します。権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

vSphere Client での権限名	説明	必要とするオブジェクト	API での権限名
ディスクの廃止操作を許可	データ ストアの運用を終了できるようにします。	データストア	Namespaces.ManageDisks
ワークロード コンポーネント ファイルのバックアップ	etcd クラスタのコンテンツをバックアップできるようにします (VMware Cloud on AWS でのみ使用)。	クラスタ	Namespaces.Backup
アクセス可能な名前空間の一覧表示	アクセス可能な vSphere 名前空間 を一覧表示できます。	クラスタ	Namespaces.ListAccess
クラスタ全体の構成の変更	スーパーバイザー の構成の変更、および vSphere 名前空間の作成と削除を行うことができます。	クラスタ	Namespaces.ManageCapabilities
クラスタ全体での名前空間のセルフサービス構成の変更	vSphere 名前空間 のセルフサービス構成を変更できます。	クラスタ (アクティブ化および非アクティブ化用) テンプレート (構成の変更用) vCenter Server (テンプレートの作成用)	Namespaces.SelfServiceManage
名前空間構成の変更	vSphere 名前空間 の構成オプション (リソースの割り当て、ユーザーの権限、コンテンツ ライブラリの関連付けなど) を変更できます。	クラスタ	Namespaces.Manage
クラスタ機能の切り替え	クラスタ スーパーバイザー の機能の状態を操作できます (VMware Cloud on AWS でのみ内部で使用)。	クラスタ	なし
クラスタを新しいバージョンにアップグレード	スーパーバイザー のアップグレードを開始できます。	クラスタ	Namespaces.Upgrade

スーパーバイザー サービス の権限

スーパーバイザー サービス の権限は、vSphere IaaS control plane 環境で スーパーバイザー サービス を作成および管理できるユーザーを制御します。

表 1-1. スーパーバイザー サービス の権限

vSphere Client での権限名	説明	必要とするオブジェクト	API での権限名
スーパーバイザー サービスの管理	スーパーバイザー サービス を作成、更新、または削除できるようにします。また、スーパーバイザー への スーパーバイザー サービス のインストール、およびスーパーバイザー サービス バージョンの作成または削除を許可します。	クラスタ	SupervisorServices.Manage

仮想マシン クラスの権限

仮想マシン クラスの権限は、vSphere 名前空間 で仮想マシン クラスを追加および削除できるユーザーを制御します。

表 1-2. 仮想マシン クラスの権限

vSphere Client での権限名	説明	必要とするオブジェクト	API での権限名
仮想マシン クラスの管理	スーパーバイザー 上の vSphere 名前空間 で仮想マシン クラスを管理できます。	クラスタ	VirtualMachineClasses.Manage

ストレージ ビュー権限

ストレージ ビュー権限を使用すると、vCenter Server でストレージ ポリシーを表示して、vSphere 名前空間 に割り当てることができます。

表 1-3. ストレージ ビュー権限

vSphere Client での権限名	説明	必要とするオブジェクト	API での権限名
サービスの構成	権限のあるユーザーに対してすべてのストレージ監視サービス API の使用を許可します。読み取り専用のストレージ監視サービス API に対する権限では、ストレージ ビュー.表示 を使用します。	ルート vCenter Server	StorageViews.ConfigureService
表示	権限のあるユーザーに対して読み取り専用のストレージ監視サービス API の使用を許可します。	ルート vCenter Server	StorageViews.View

vSphere IaaS control plane セキュリティ

vSphere IaaS control plane は vSphere のセキュリティ機能を利用して、デフォルトで安全な Tanzu Kubernetes Grid クラスタをプロビジョニングします。

vSphere IaaS control plane は、vCenter Server および ESXi に組み込まれたセキュリティ機能を利用できる、vSphere に対するアドオン モジュールです。詳細については、vSphere Security ドキュメントを参照してください。

スーパーバイザー は、データベース (etcd) に保存されているすべてのシークレットを暗号化します。シークレットは、起動時に vCenter Server によって提供されるローカル暗号化キー ファイルを介して暗号化されます。復号キーは スーパーバイザー ノードのメモリ (tempfs) に格納されるほかに、vCenter Server データベース内のディスクに暗号化形式で格納されます。各システムの root ユーザーは、復号キーをクリア テキストで入手できます。各ワークロード クラスタのデータベース内に保持されているシークレットは、クリア テキスト形式で保存されます。すべての etcd 接続は、インストール時に生成され、アップグレード中にローテーションされる証明書を使用して認証されます。現在、証明書を手動でローテーションまたは更新することはできません。同じ暗号化モデルは、各 Tanzu Kubernetes Grid クラスタの制御プレーンにインストールされているデータベース (etcd) 内のデータに適用されます。

スーパーバイザー では、互換性のあるシステムで機密性の高い vSphere ポッド を実行できます。機密性の高い vSphere ポッド を作成するには、セキュリティ拡張機能として Secure Encrypted Virtualization-Encrypted State (SEV-ES) を追加します。詳細については、『vSphere IaaS 制御プレーンのサービスとワークロード』の機密性の確保された vSphere ポッドのデプロイを参照してください。

Tanzu Kubernetes Grid クラスタはデフォルトでセキュリティ保護されています。すべての Tanzu Kubernetes Grid クラスタで、制限付き PodSecurityPolicy (PSP) を使用できます。開発者が特権ポッドまたはルート コンテナを実行する必要がある場合、クラスタ管理者は、最低でも、デフォルトの特権 PSP へのユーザー アクセスを許可するロールバインドを作成する必要があります。詳細については、『vSphere IaaS 制御プレーンでの TKG サービスの使用』を参照してください。

Tanzu Kubernetes Grid クラスタにはインフラストラクチャ認証情報がありません。Tanzu Kubernetes Grid クラスタ内に保存される認証情報では、Tanzu Kubernetes Grid クラスタにテナントのある vSphere 名前空間にのみアクセスが可能です。そのため、クラスタ オペレータまたはユーザーの権限のエスカレーションが行われることはありません。

Tanzu Kubernetes Grid クラスタへのアクセスに使用される認証トークンは、スーパーバイザー または他の Tanzu Kubernetes Grid クラスタへのアクセスに使用できないように範囲が設定されます。これにより、クラスタ オペレータ、またはクラスタを侵害する可能性があるユーザーは、Tanzu Kubernetes Grid クラスタにログインするときに、root レベルのアクセス権を使用して vSphere 管理者のトークンをキャプチャできなくなります。

スーパーバイザー アーキテクチャおよびコンポーネント

2

vSphere IaaS control plane が有効になっているクラスタは、スーパーバイザーと呼ばれます。3 つの vSphere クラスタで 1 つのスーパーバイザーを有効にする 3 ゾーンのデプロイから選択することも、vSphere クラスタとスーパーバイザー間の 1 対 1 のマッピングを選択することもできます。スーパーバイザーは、vSphere ポッド、仮想マシン、および Tanzu Kubernetes Grid クラスタが含まれているワークロードの実行に必要なコンポーネントとリソースを提供する vSphere IaaS control plane の基盤です。

次のトピックを参照してください。

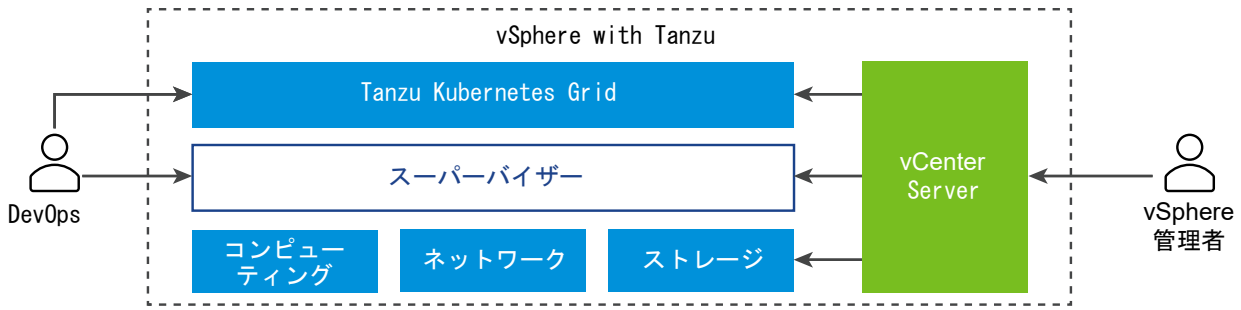
- スーパーバイザー アーキテクチャ
- スーパーバイザー ネットワーク
- スーパーバイザー ストレージ

スーパーバイザー アーキテクチャ

vSphere クラスタで vSphere IaaS control plane を有効にして、そのクラスタが スーパーバイザー になると、ハイパーバイザー レイヤー内に Kubernetes 制御プレーンが作成されます。このレイヤーには、ESXi 内で Kubernetes ワークロードを実行する機能を有効にする特定のオブジェクトが含まれています。

図 2-1. スーパーバイザー の一般的なアーキテクチャ

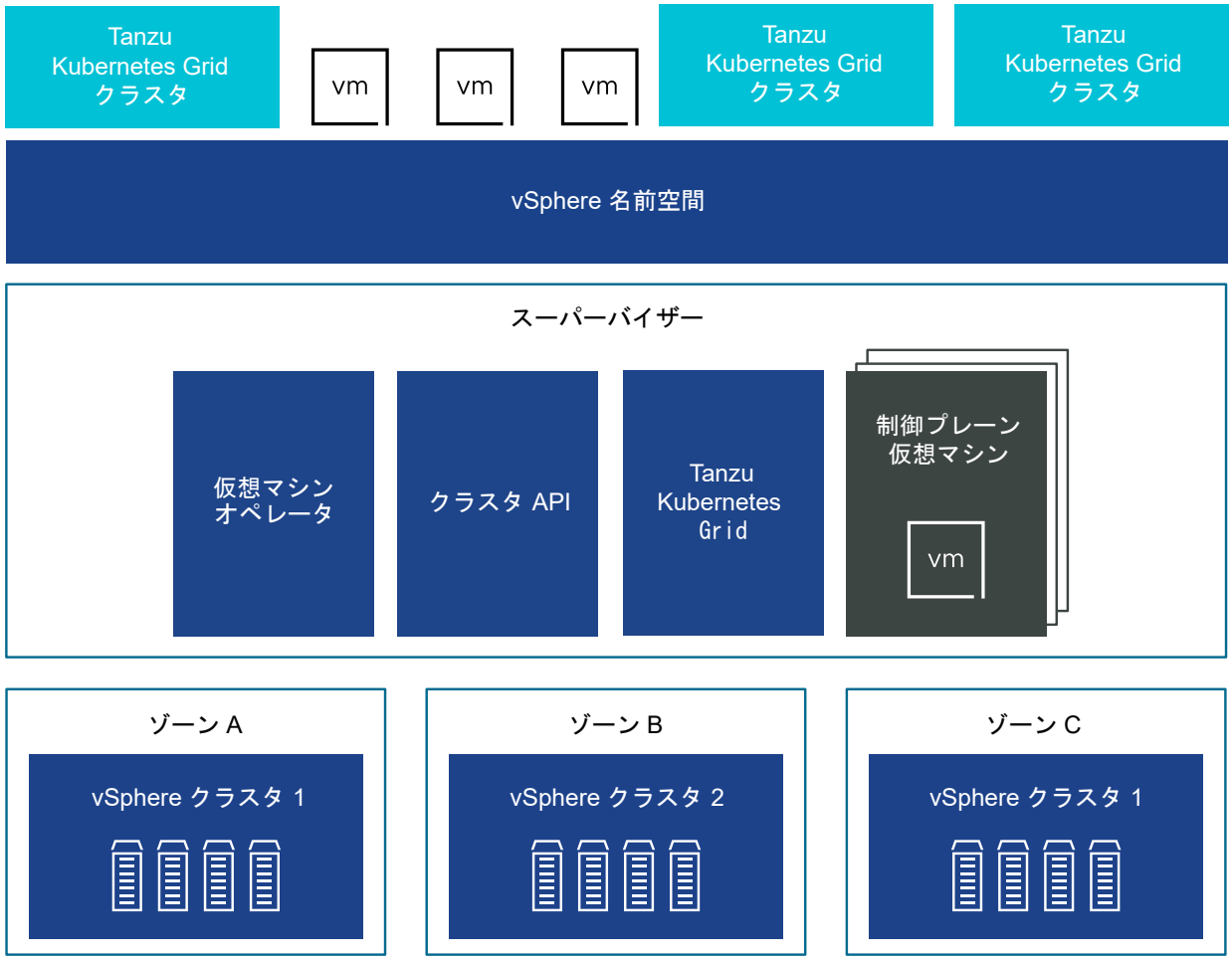
この図は、Tanzu Kubernetes Grid が上、スーパーバイザー が中間、ESXi、ネットワーク、およびストレージが下に配置され、vCenter Server によって管理されている、vSphere IaaS control plane アーキテクチャの概要を示しています。



スーパーバイザー は、コンピューティング用の ESXi、NSX または Distributed Switch ネットワーク、および vSAN または他の共有ストレージ ソリューションで構成される Software-Defined Data Center (SDDC) レイヤー上で実行されます。共有ストレージは、vSphere ポッド のパーシステント ボリューム、スーパーバイザー 内で実行される仮想マシン、および Tanzu Kubernetes Grid クラスタ内のポッドに使用されます。スーパーバイザー を作成したら、vSphere 管理者は、スーパーバイザー 内に vSphere 名前空間 と呼ばれる名前空間を作成できます。DevOps エンジニアは、vSphere ポッド 内で動作しているコンテナで構成されたワークロードを実行し、仮想マシン サービスを使用して仮想マシンをデプロイし、Tanzu Kubernetes Grid クラスタを作成することができます。

スーパーバイザー を 3 つの vSphere Zone にデプロイすると、クラスタレベルの障害に対して Kubernetes ワークロードを保護するクラスタレベルの高可用性を提供できます。vSphere Zone は、独立した障害ドメインとして設定できる 1 つの vSphere クラスタにマッピングされます。3 ゾーンのデプロイでは、3 つの vSphere クラスタがすべて 1 つの スーパーバイザー になります。スーパーバイザー を 1 つの vSphere クラスタにデプロイすることもできます。これにより、すでにゾーンにマッピングされている vSphere クラスタを使用しない限り、vSphere Zone が自動的に作成され、クラスタにマッピングされます。単一クラスタのデプロイの場合、スーパーバイザー では、vSphere HA によって提供される高可用性がホスト レベルでのみ確保されます。

図 2-2. 3 ゾーンのスーパーバイザーのアーキテクチャ

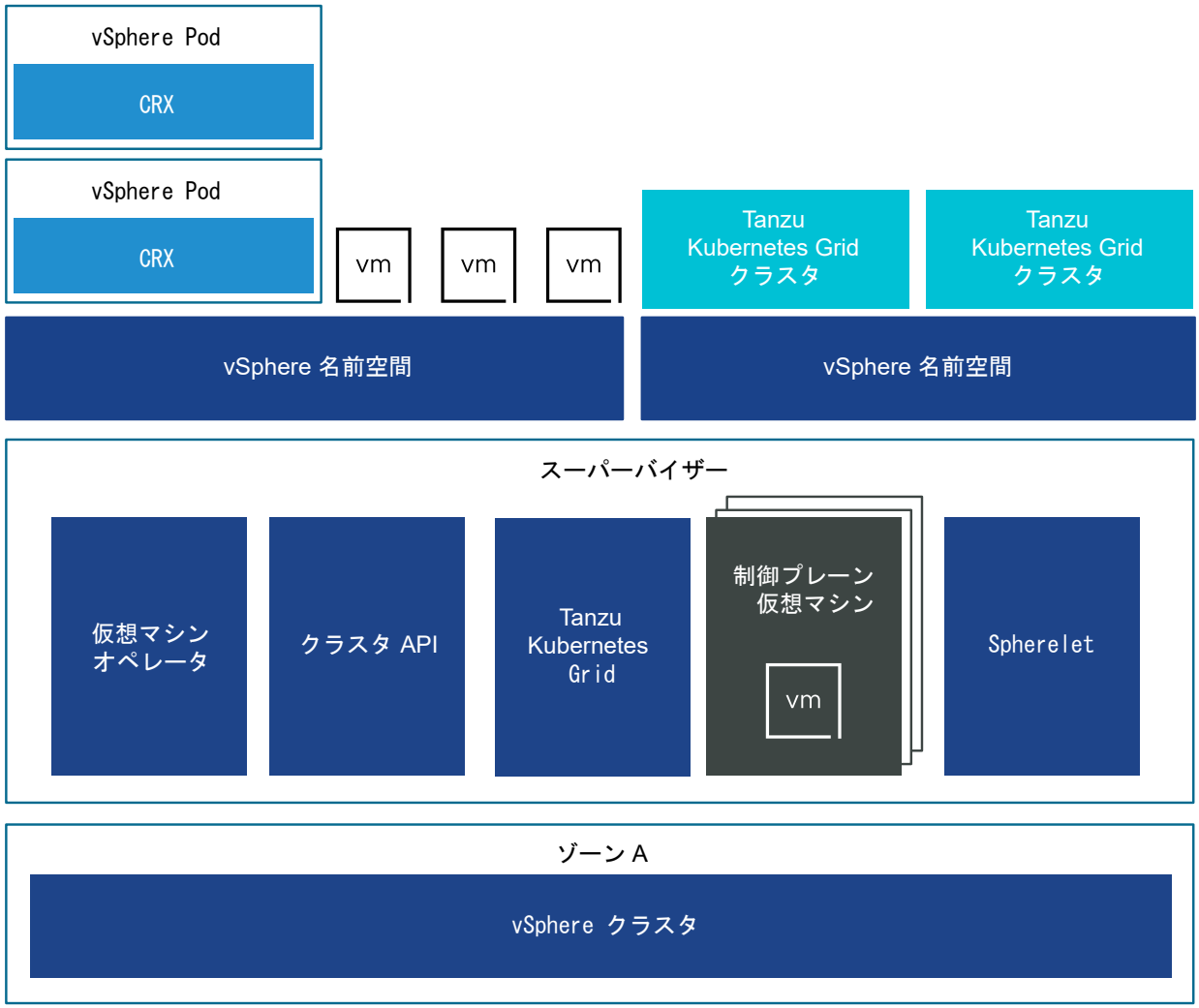


3 ゾーンの スーパーバイザー では、仮想マシン サービスを使用して作成された Tanzu Kubernetes Grid クラスタと仮想マシンで Kubernetes ワークロードを実行できます。3 ゾーンの スーパーバイザー には、次のコンポーネントがあります。

- スーパーバイザー 制御プレーン仮想マシン。スーパーバイザー には、合計 3 台の スーパーバイザー 制御プレーン仮想マシンが作成されます。3 ゾーンのデプロイでは、各ゾーンに 1 台の制御プレーン仮想マシンが配置されます。3 台の スーパーバイザー 制御プレーン仮想マシンにはそれぞれ独自の IP アドレスがあるため、ロードバランシングが行われます。また、フローティング IP アドレスが仮想マシンのうち 1 台に割り当てられ、5 番目の IP アドレスがパッチ適用の目的で予約されます。vSphere DRS は、スーパーバイザー の ESXi ホスト部分の制御プレーン仮想マシンの正確な配置を決定し、必要に応じて移行します。
- Tanzu Kubernetes Grid とクラスタ API。スーパーバイザー で実行されるモジュールです。Tanzu Kubernetes Grid クラスタのプロビジョニングと管理を有効にします。
- 仮想マシン サービス。スタンドアローン仮想マシンと Tanzu Kubernetes Grid クラスタを構成する仮想マシンをデプロイして、実行するモジュールです。

3 ゾーンの スーパーバイザー では、ゾーンにマッピングされた各 vSphere クラスタに名前空間リソース プールが作成されます。名前空間は、各ゾーン内の 3 つの vSphere クラスタすべてに分散されます。3 ゾーンの スーパーバイザー の名前空間に使用されるリソースは、基盤となる 3 つのすべての vSphere クラスタから均等に取得されます。たとえば、300 MHz の CPU を使用する場合は、各 vSphere クラスタから 100 MHz が取得されます。

図 2-3. 単一クラスタのスーパーバイザーのアーキテクチャ



単一の vSphere クラスタにデプロイされる スーパーバイザー にも、クラスタの ESXi ホスト部分に配置された 3 台の制御プレーン仮想マシンがあります。単一クラスタの スーパーバイザー では、Tanzu Kubernetes Grid クラスタと仮想マシンに加えて vSphere ポッド を実行できます。vSphere DRS は、スーパーバイザー 制御プレーン仮想マシンの Kubernetes スケジューラと統合されているため、DRS によって vSphere ポッド の配置が決まります。DevOps エンジニアとして vSphere ポッド をスケジュール設定すると、その要求は通常の Kubernetes ワークフローを経由して DRS に送信され、そこで最終的な配置が決定されます。

vSphere ポッド のサポートにより、単一クラスタの スーパーバイザー には次の追加コンポーネントが含まれます。

- Spherelet。各ホストに Spherelet と呼ばれる追加のプロセスが作成されます。このプロセスは、ESXi に対してネイティブに移植された kubelet であり、このプロセスによって ESXi ホストは Kubernetes クラスタのメンバーになることができます。

- Container Runtime Executive (CRX) コンポーネント。hostd と vCenter Server の観点から見ると、CRX は仮想マシンと似ています。CRX には、ハイパーバイザーと連携する準仮想化 Linux カーネルが含まれています。CRX は仮想マシンと同じハードウェア仮想化技術を使用しており、仮想マシンの境界で囲まれています。直接起動の技法が使用されるため、CRX の Linux ゲストは、カーネルの初期化を経由することなくメインの init プロセスを開始できます。これにより、vSphere ポッド がコンテナとほぼ同じ速度で起動できるようになります。

スーパーバイザー ネットワーク

vSphere IaaS control plane 環境の場合、スーパーバイザー は vSphere ネットワーク スタックまたは NSX を使用して、スーパーバイザー 制御プレーンの仮想マシン、サービス、およびワークロードへの接続を提供できます。

スーパーバイザー に vSphere ネットワーク スタックが構成されている場合、スーパーバイザー のすべてのホストは、ワークロードと スーパーバイザー 制御プレーン仮想マシンへの接続を提供する Distributed Switch に接続されます。vSphere ネットワーク スタックを使用する スーパーバイザー には、DevOps ユーザーおよび外部サービスへの接続を提供するために vCenter Server 管理ネットワーク上にロード バランサが必要です。

NSX を使用して構成される スーパーバイザー は、ソリューションのソフトウェアベースのネットワークと NSX Edge ロード バランサまたは NSX Advanced Load Balancer を使用して、外部サービスと DevOps ユーザーへの接続を提供します。環境が次の条件を満たしている場合は、NSX で NSX Advanced Load Balancer を構成できます。

- NSX のバージョンが 4.1.1 以降である。
- NSX Advanced Load Balancer バージョンが 2.1.4 以降で、Enterprise ライセンスがある。
- 構成する NSX Advanced Load Balancer Controller が NSX に登録されている。
- NSX ロード バランサが スーパーバイザー でまだ構成されていない。

VDS を使用した スーパーバイザー ネットワーク

ネットワーク スタックとしての VDS によってバッキングされている スーパーバイザー では、スーパーバイザー をバッキングしている vSphere クラスタのすべてのホストが同じ VDS に接続されている必要があります。スーパーバイザー は、Kubernetes ワークロードおよび制御プレーン トラフィックのワークロード ネットワークとして分散ポート グループを使用します。ワークロード ネットワークを スーパーバイザー 内の名前空間に割り当てます。

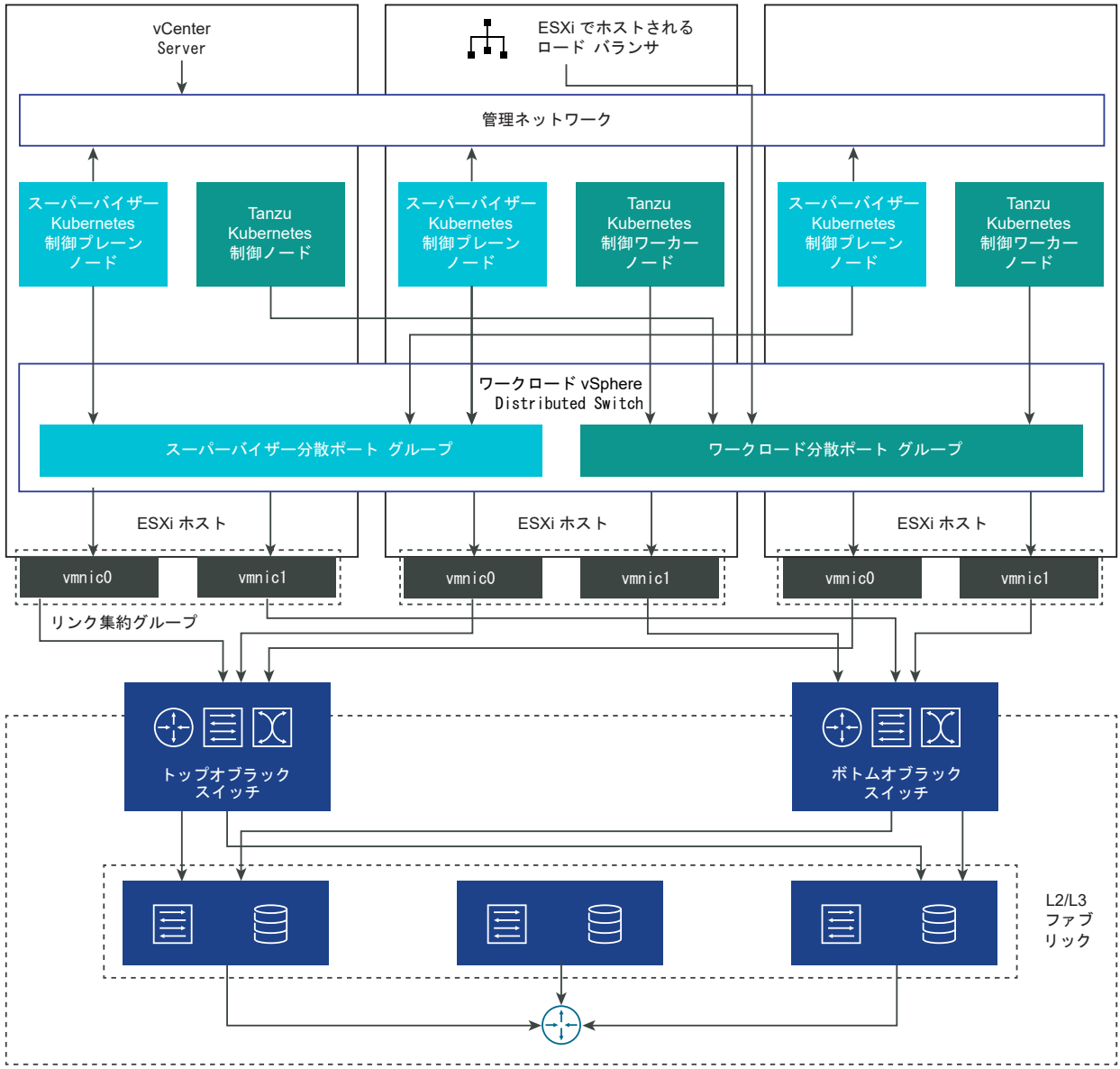
スーパーバイザー に実装するトポロジによっては、1 つ以上の分散ポート グループをワークロード ネットワークとして使用できます。スーパーバイザー 制御プレーン仮想マシンへの接続を提供するネットワークは、プライマリ ワークロード ネットワークと呼ばれます。スーパーバイザー 上のすべての名前空間にこのネットワークを割り当てることも、名前空間ごとに異なるネットワークを使用することもできます。クラスタが配置されている名前空間に割り当てられたワークロード ネットワークに、Tanzu Kubernetes Grid クラスタが接続されます。

VDS によってバッキングされる スーパーバイザー は、DevOps ユーザーと外部サービスへの接続を提供するためにロード バランサを使用します。NSX Advanced Load Balancer または HAProxy ロード バランサを使用できます。

詳細については、NSX Advanced Load Balancer のインストールと構成および HAProxy ロード バランサのインストールと構成を参照してください。

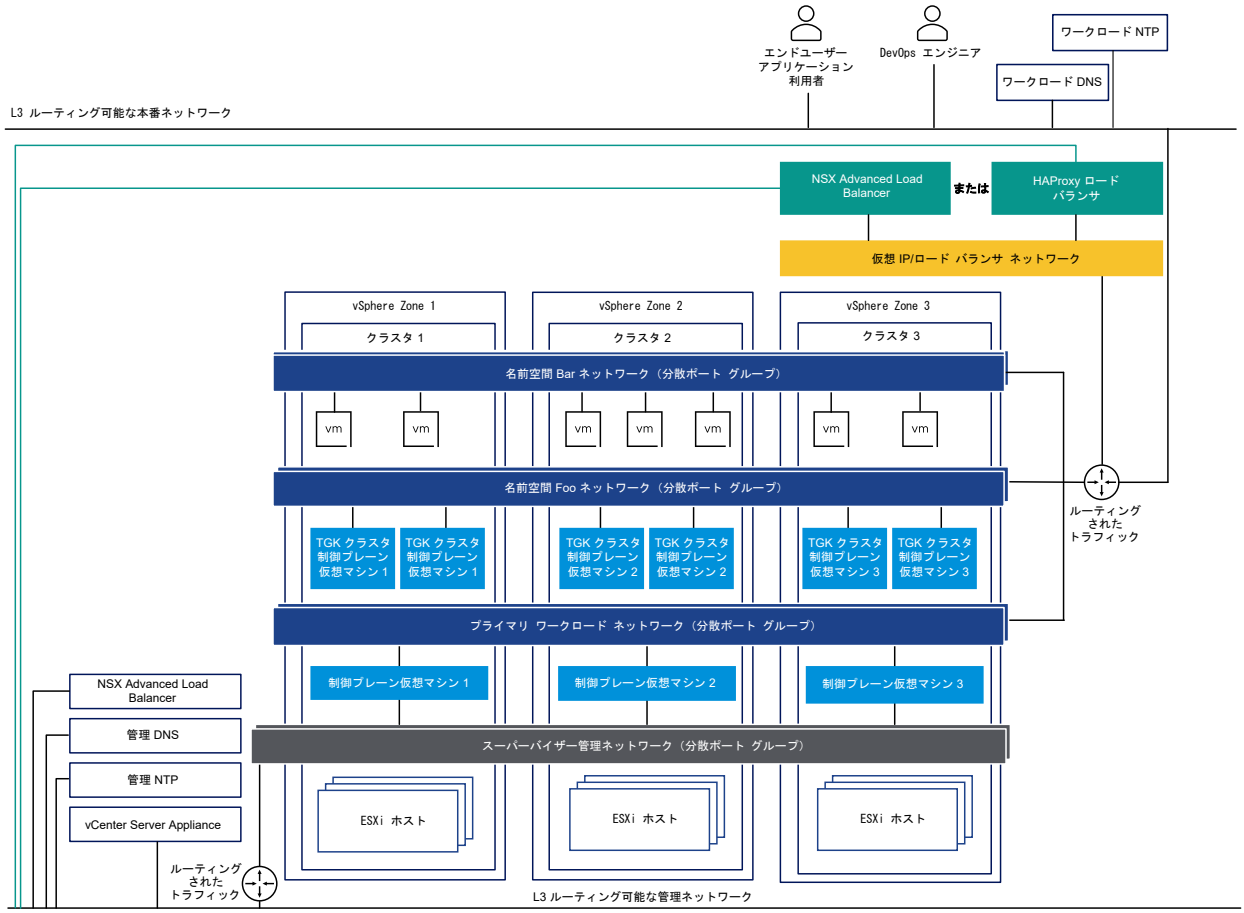
単一クラスタ スーパーバイザー セットアップでは、スーパーバイザー は 1 つの vSphere クラスタのみによってバッキングされます。クラスタのすべてのホストが、VDS に接続されている必要があります。

図 2-4. VDS を使用した単一クラスタ スーパーバイザー ネットワーク



3 ゾーン スーパーバイザー では、スーパーバイザー を 3 つの vSphere ゾーンにデプロイします。それぞれのゾーンは、vSphere クラスタにマッピングされています。これらの vSphere クラスタのすべてのホストは、同じ VDS に接続されている必要があります。すべての物理サーバが L2 デバイスに接続されている必要があります。名前空間に構成するワークロード ネットワークは、3 つの vSphere ゾーンすべてにまたがります。

図 2-5. VDS を使用した 3 ゾーン スーパーバイザー ネットワーク



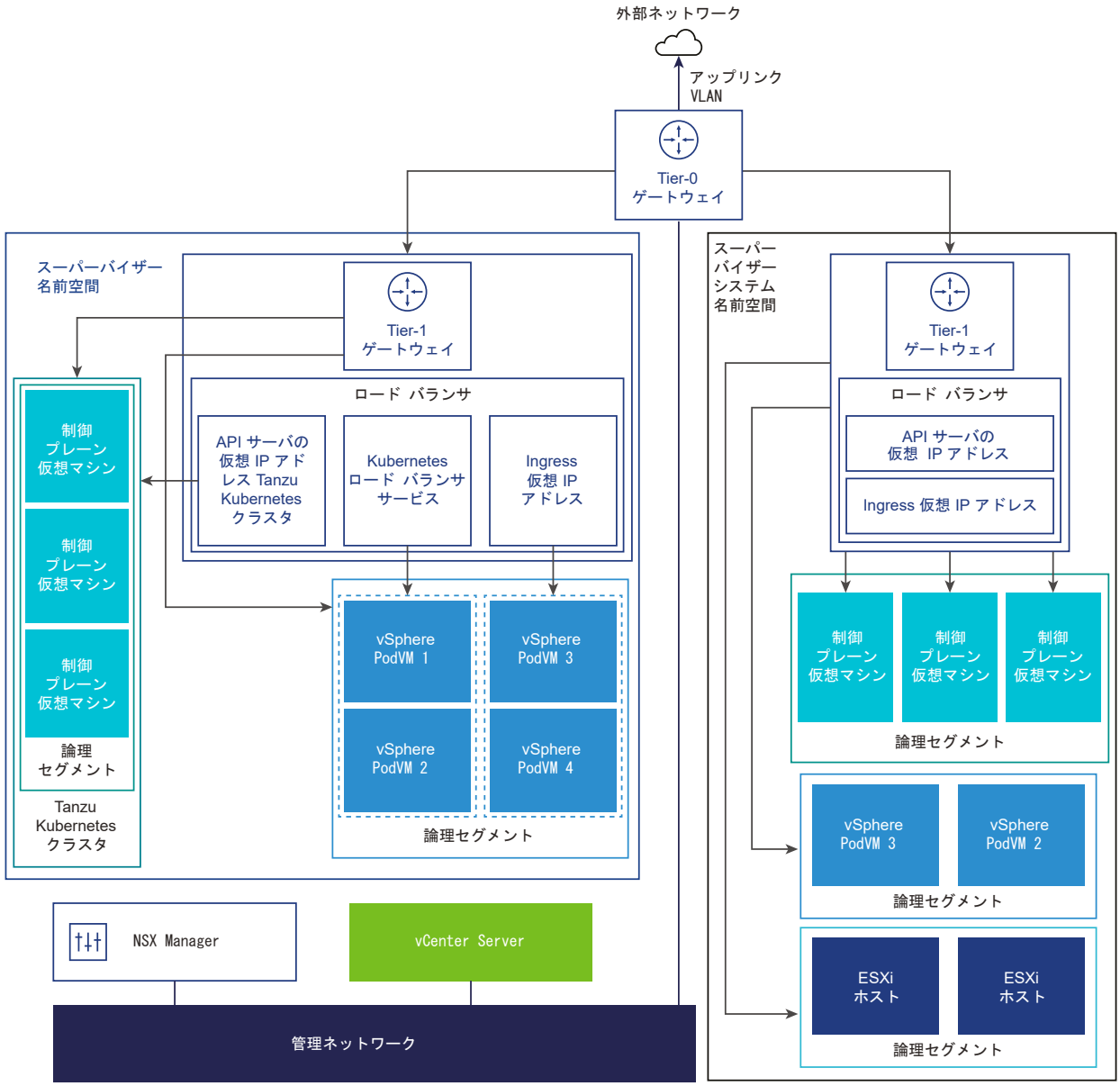
NSX を使用する スーパーバイザー ネットワーク

NSX は、スーパーバイザー 内のオブジェクトおよび外部ネットワークへのネットワーク接続を提供します。クラスタを構成する ESXi ホストへの接続は、標準の vSphere ネットワークによって処理されます。

既存の NSX デプロイを使用するか、NSX の新しいインスタンスをデプロイすることによって、スーパーバイザー ネットワークを手動で構成することもできます。

詳細については、「vSphere IaaS control plane で使用する NSX のインストールと構成」を参照してください。

図 2-6. NSX を使用する スーパーバイザー ネットワーク



- NSX Container Plugin (NCP) は NSX と Kubernetes を統合します。NCP のメイン コンポーネントはコンテナで実行され、NSX Manager および Kubernetes 制御プレーンと通信します。NCP は、コンテナおよびその他のリソースへの変更を監視し、NSX API を呼び出して、コンテナの論理ポート、セグメント、ルーター、セキュリティ グループなどのネットワーク リソースを管理します。

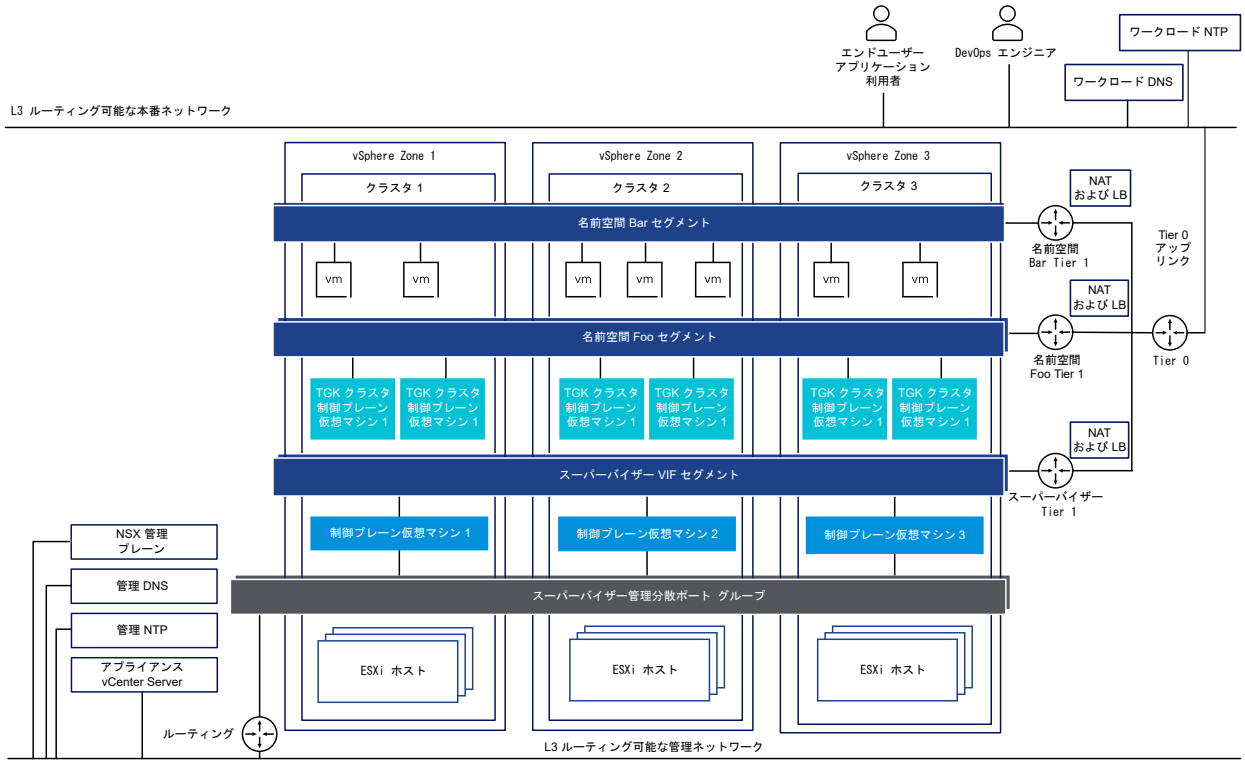
  NCP はデフォルトで、システム名前空間用の共有 Tier-1 ゲートウェイを 1 つ作成し、名前空間ごとに Tier-1 ゲートウェイとロード バランサを 1 つずつ作成します。Tier-1 ゲートウェイは、Tier-0 ゲートウェイとデフォルトのセグメントに接続されています。

  システム名前空間は、スーパーバイザー クラスタと Tanzu Kubernetes Grid クラスタの機能に不可欠な主要コンポーネントで使用される名前空間です。Tier-1 ゲートウェイ、ロード バランサ、SNAT IP を含む共有ネットワーク リソースは、システム名前空間内でグループ化されます。

- NSX Edge は、外部ネットワークから スーパーバイザー オブジェクトへの接続を提供します。NSX Edge クラスタには、スーパーバイザー 制御プレーン仮想マシン上にある Kubernetes API サーバの冗長性を確保するロード バランサや、スーパーバイザー の外部に公開されてアクセスできる必要があるアプリケーションがあります。
- NSX Edge クラスタには Tier-0 ゲートウェイが関連付けられており、外部ネットワークへのルーティングを提供します。アップリンク インターフェイスでは、動的ルーティング プロトコルの BGP またはスタティック ルーティングのいずれかが使用されます。
- 各 vSphere 名前空間 には、個別のネットワークのほかに、Tier-1 ゲートウェイ、ロード バランサ サービス、SNAT IP アドレスなど、名前空間内のアプリケーションで共有される一連のネットワーク リソースが含まれています。
- 同じ名前空間内にある vSphere ポッド、通常の仮想マシン、または Tanzu Kubernetes Grid クラスタで実行されるワークロードは、North-South 接続に対して同じ SNAT IP アドレスを共有します。
- vSphere ポッド または Tanzu Kubernetes Grid クラスタで実行されるワークロードには、デフォルトのファイアウォールによって実装される共通の隔離ルールが適用されます。
- Kubernetes 名前空間ごとに個別の SNAT IP アドレスが必要になることはありません。名前空間の間の East-West 接続は、SNAT ではありません。
- 各名前空間のセグメントは、NSX Edge クラスタに関連付けられている、標準モードで機能する VDS に配置されます。このセグメントは、スーパーバイザー にオーバーレイ ネットワークを提供します。
- スーパーバイザー の共有 Tier-1 ゲートウェイ内に、個別のセグメントがあります。各 Tanzu Kubernetes Grid クラスタのセグメントは、名前空間の Tier-1 ゲートウェイ内で定義されています。
- 各 ESXi ホストの Spherelet プロセスは、管理ネットワーク上のインターフェイスを介して vCenter Server と通信します。

ネットワーク スタックとして NSX を使用して構成された 3 ゾーン スーパーバイザー では、ゾーンにマッピングされた 3 つのすべての vSphere クラスタのすべてのホストが、同じ VDS に接続され、同じ NSX オーバーレイ トランスポート ゾーンに参加している必要があります。すべてのホストが同じ L2 物理デバイスに接続されている必要があります。

図 2-7. NSX を使用した 3 ゾーン スーパーバイザー ネットワーク



NSX と NSX Advanced Load Balancer を使用する スーパーバイザー ネットワーク

NSX は、スーパーバイザー 内のオブジェクトおよび外部ネットワークへのネットワーク接続を提供します。NSX を使用して構成される スーパーバイザー では、NSX Edge または NSX Advanced Load Balancer を使用できます。

NSX Advanced Load Balancer のコンポーネントには、NSX Advanced Load Balancer Controller クラスタ、サービス エンジン（データ プレーン）仮想マシン、Avi Kubernetes Operator (AKO) が含まれます。

NSX Advanced Load Balancer Controller は vCenter Server と連携して、Tanzu Kubernetes Grid クラスタのロード バランシングを自動実行します。コントローラは、サービス エンジンのプロビジョニング、サービス エンジン間でのリソースの調整、サービス エンジンのメトリックとログの集計を行います。また、ユーザー操作およびプログラムによる連携のための Web インターフェイス、コマンドライン インターフェイス、および API を提供します。コントローラ仮想マシンをデプロイして構成した後、コントローラ クラスタをデプロイして、HA 用の制御プレーン クラスタを設定できます。

サービス エンジンはデータ プレーン仮想マシンです。サービス エンジンは 1 つ以上の仮想サービスを実行します。サービス エンジンは NSX Advanced Load Balancer Controller によって管理されます。コントローラは、仮想サービスをホストするようにサービス エンジンをプロビジョニングします。

サービス エンジンには、次の 2 種類のネットワーク インターフェイスがあります。

- 仮想マシンの最初のネットワーク インターフェイス `vnic0` は管理ネットワークに接続され、そこから NSX Advanced Load Balancer Controller に接続することができます。

- もう一方のインターフェイス `vnic1 - 8` は、仮想サービスが実行されるワークロード ネットワークに接続されます。

サービス エンジン インターフェイスは、適切な Distributed Switch ポート グループに自動的に接続します。各サービス エンジンは、最大 1,000 個の仮想サービスをサポートできます。

仮想サービスは、Tanzu Kubernetes Grid クラスタ ワークロード用のレイヤー 4 およびレイヤー 7 ロード バランシング サービスを提供します。仮想サービスは、1 つの仮想 IP アドレスと複数のポートで構成されます。仮想サービスをデプロイすると、コントローラによって ESX サーバが自動的に選択され、サービス エンジンが起動して適切なネットワーク（ポート グループ）に接続します。

最初のサービス エンジンは、最初の仮想サービスが構成された後にのみ作成されます。以降に構成された仮想サービスは、既存のサービス エンジンを使用します。

各仮想サーバは、Tanzu Kubernetes Grid クラスタのロード バランサ タイプの異なる IP アドレスを持つレイヤー 4 ロード バランサを公開します。各仮想サーバに割り当てられる IP アドレスは、構成時にコントローラに指定する IP アドレス ブロックから選択されます。

Avi Kubernetes Operator (AKO) は Kubernetes リソースを監視し、NSX Advanced Load Balancer Controller と通信して、対応するロード バランシング リソースを要求します。Avi Kubernetes Operator は、有効化プロセスの一環として スーパーバイザー にインストールされます。

詳細については、「NSX および NSX Advanced Load Balancer のインストールと構成」を参照してください。

図 2-8. NSX と NSX Advanced Load Balancer Controller を使用する スーパーバイザー ネットワーク

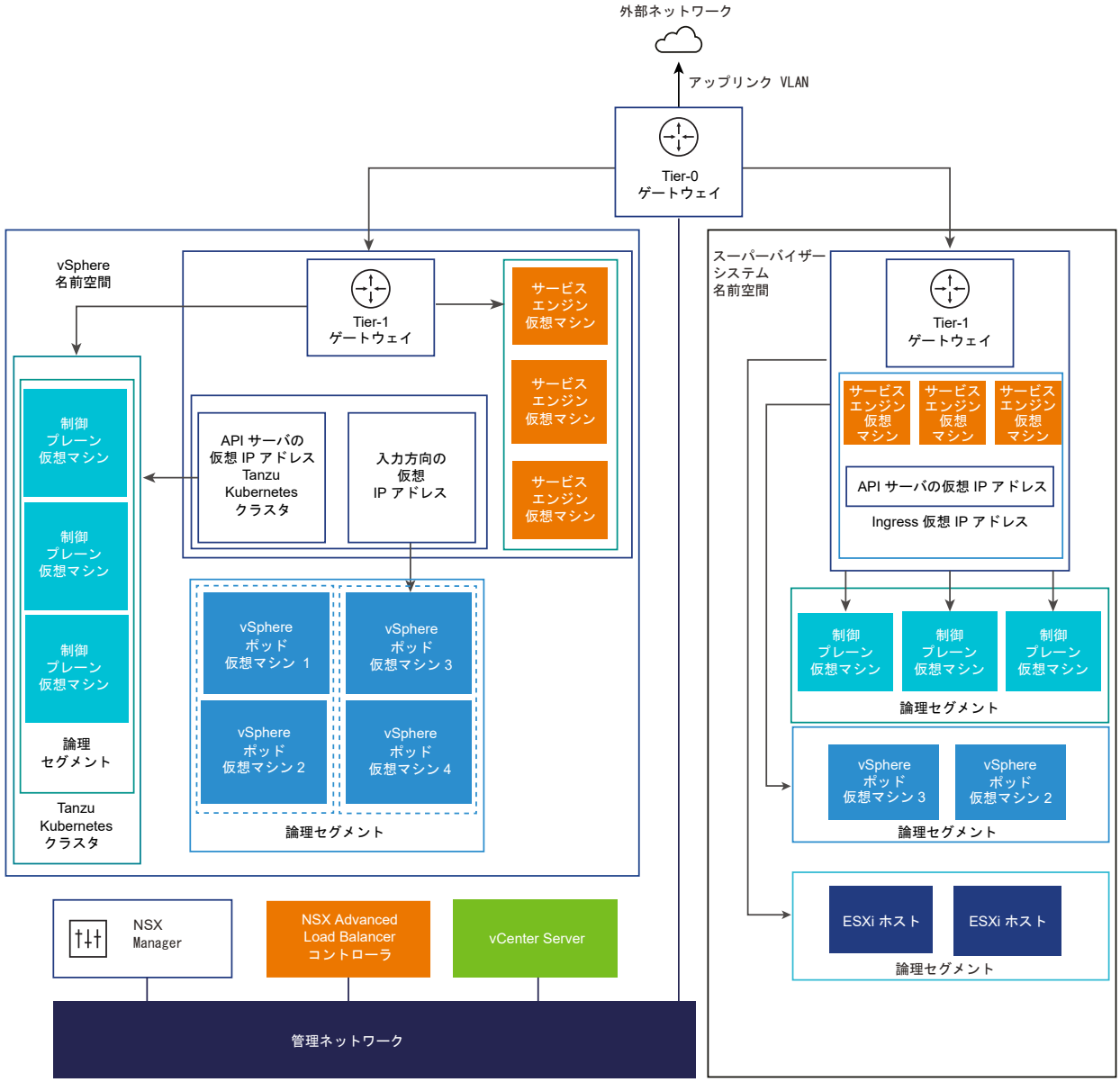
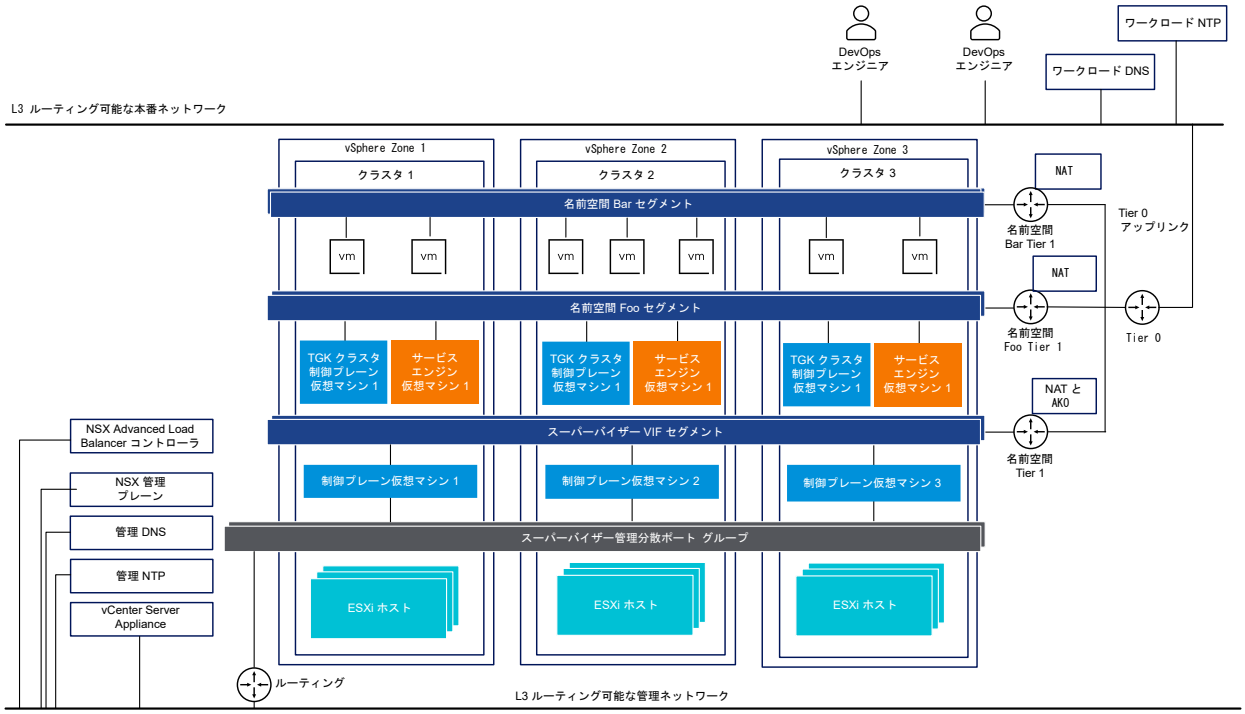


図 2-9. NSX と NSX Advanced Load Balancer Controller を使用した 3 ゾーン スーパーバイザー ネットワーク



重要： NSX のデプロイで NSX Advanced Load Balancer Controller を構成する場合は、次の点を考慮してください。

- vCenter Server 拡張リンク モード デプロイでは NSX Advanced Load Balancer Controller をデプロイできません。単一の vCenter Server のデプロイでのみ NSX Advanced Load Balancer Controller をデプロイできます。複数の vCenter Server がリンクされている場合、NSX Advanced Load Balancer Controller の構成時に使用できるのはそのうちの 1 つのみです。
- 多層の Tier-0 トポロジでは、NSX Advanced Load Balancer Controller を構成できません。NSX 環境が多層の Tier-0 トポロジで設定されている場合、NSX Advanced Load Balancer Controller の構成時に使用できる Tier-0 ゲートウェイは 1 つのみです。

NSX を使用するネットワークの構成方法

スーパーバイザー は、固定型ネットワーク構成を使用します。NSX を使用する スーパーバイザー ネットワークを構成するには次の 2 つの方法があり、いずれの場合でも 1 ゾーン スーパーバイザー 用の同じネットワーク モデルがデプロイされます。

- スーパーバイザー ネットワークを構成する最も簡単な方法は、VMware Cloud Foundation SDDC Manager を使用することです。詳細については、VMware Cloud Foundation SDDC Manager のドキュメントを参照してください。詳細については、『VMware Cloud Foundation 管理ガイド』を参照してください。

- 既存の NSX デプロイを使用するか、NSX の新しいインスタンスをデプロイすることによって、スーパーバイザー ネットワークを手動で構成することもできます。詳細については、「vSphere IaaS control plane で使用する NSX のインストールと構成」を参照してください。

スーパーバイザー ストレージ

スーパーバイザー のコンポーネント、アプリケーション、およびワークロードは、データを保存して取得する必要があります。アプリケーションやオブジェクトによって、一時的な高速ストレージを使用する場合と、永続的なストレージが必要な場合があります。

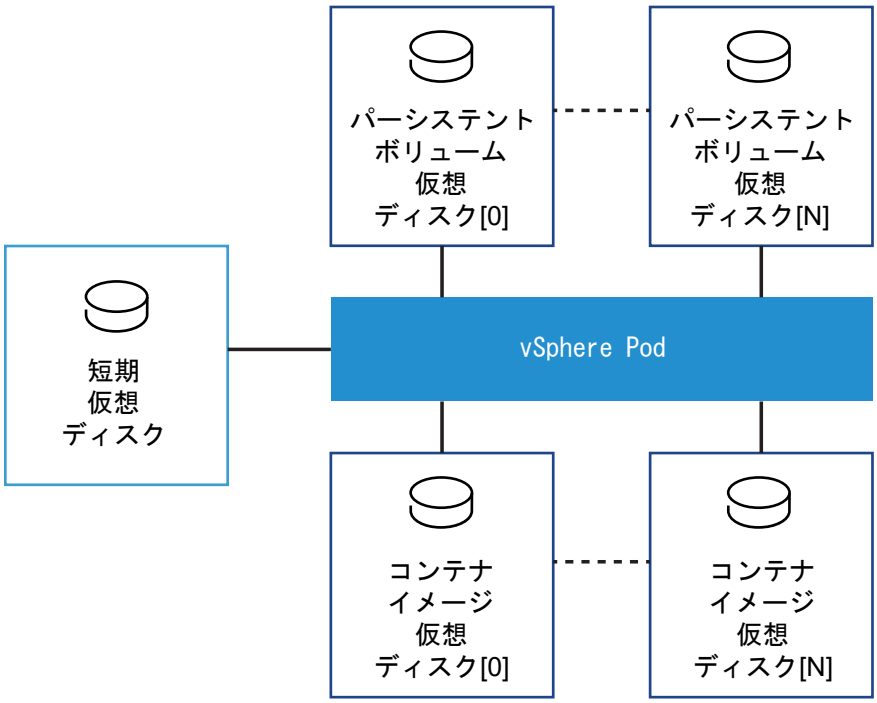
ストレージ ポリシーについて

スーパーバイザー は、ストレージ ポリシーを使用して、vSphere 環境内で使用可能なストレージと統合します。このポリシーは、データストアを表し、制御プレーン仮想マシン、vSphere ポッド の短期ディスク、コンテナ イメージなどのコンポーネントやオブジェクトのストレージ配置を管理します。パーシステント ボリュームおよび仮想マシン コンテンツ ライブラリのストレージ配置にもポリシーが必要になることがあります。Tanzu Kubernetes Grid クラスタを使用する場合は、ストレージ ポリシーによって、Tanzu Kubernetes Grid クラスタ ノードのデプロイ方法も決定されます。

ストレージ ポリシーは、VMFS、NFS、vSAN（vSAN ESA を含む）、vVol など、環境内のすべての共有データストアをサポートします。

vSphere ストレージ環境と DevOps のニーズに応じて、さまざまなストレージ クラスのために複数のストレージ ポリシーを作成することができます。スーパーバイザー を有効にして名前空間を設定すると、多様なオブジェクト、コンポーネント、ワークロードで使用されるさまざまなストレージ ポリシーを割り当てることができます。

たとえば、vSphere ポッド に 3 つのタイプの仮想ディスクがマウントされていて、vSphere ストレージ環境にブロンズ、シルバー、ゴールドの 3 つのクラスのデータストアがある場合、すべてのデータストアに対してストレージ ポリシーを作成できます。その後、短期仮想ディスクとコンテナ イメージ仮想ディスクにブロンズ データストアを使用し、パーシステント ボリューム仮想ディスクにシルバーおよびゴールド データストアを使用することができます。



ストレージ ポリシーの作成については、『vSphere IaaS 制御プレーンのインストールと構成』ドキュメントの「ストレージ ポリシーの作成」を参照してください。

ストレージ ポリシーの一般的な情報については、『vSphere のストレージ』ドキュメントのストレージ ポリシー ベースの管理の章を参照してください。

スーパーバイザー のストレージ ポリシー

スーパーバイザー レベルでは、スーパーバイザー 制御プレーン仮想マシンのストレージ ポリシーを構成します。また、デプロイで vSphere ポッド がサポートされている場合は、ストレージ ポリシーを割り当てて、短期ディスクとコンテナ イメージのデータストアの場所を指定します。スーパーバイザー を有効にする場合のストレージの設定については、『vSphere IaaS 制御プレーンのインストールと構成』ドキュメントを参照してください。ストレージ設定を変更するには、スーパーバイザーでのストレージ設定の変更を参照してください。

制御プレーン ストレージ ポリシー

このポリシーにより、制御プレーン仮想マシンが、ポリシーによって表されるデータストアに配置されます。

短期仮想ディスク

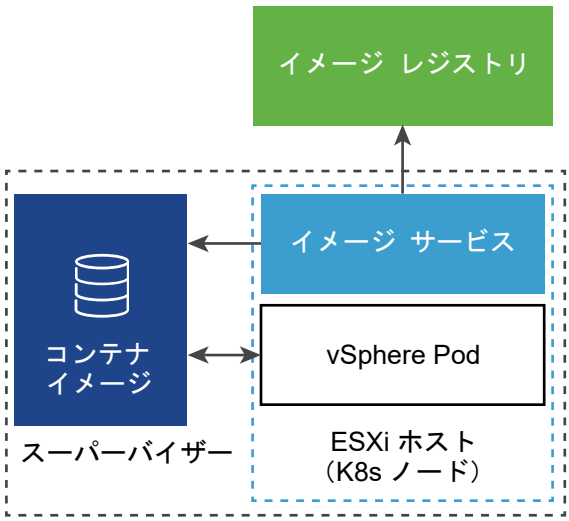
vSphere ポッド では、その動作中にログ、`emptyDir` ボリューム、`ConfigMaps` などの Kubernetes オブジェクトを保存するために、短期ストレージが必要です。この短期（一時）ストレージは、ポッドが存続する限り保持されます。短期データはコンテナの再起動後も維持されますが、ポッドのライフタイムが終了すると、短期仮想ディスクは破棄されます。

各ポッドには 1 つの短期仮想ディスクがあります。vSphere 管理者は、スーパーバイザー のストレージを構成するときに、ストレージ ポリシーを使用してすべての短期仮想ディスクのデータストアの場所を定義します。

コンテナ イメージ仮想ディスク

vSphere ポッド 内のコンテナでは、実行するソフトウェアを含むイメージを使用します。ポッドは、コンテナで使用されるイメージをイメージ仮想ディスクとしてマウントします。ポッドのライフサイクルが完了すると、イメージ仮想ディスクはポッドから接続を解除されます。

ESXi コンポーネントのイメージ サービスは、イメージ レジストリからコンテナ イメージをプルし、そのイメージをポッド内で実行される仮想ディスクに変換します。



ESXi は、ポッドで実行されているコンテナ用にダウンロードされたイメージをキャッシュできます。これ以降、同じイメージを使用するポッドは、外部コンテナ レジストリではなくローカル キャッシュからプルします。

ワークロードのパーシステント ストレージ

DevOps が名前空間で実行する特定の Kubernetes ワークロードでデータを永続的に保存するには、パーシステント ストレージが必要です。

パーシステント ストレージは、vSphere ポッド、Tanzu Kubernetes Grid クラスタ、仮想マシン、および名前空間で実行するその他のワークロードで使用できます。DevOps チームがパーシステント ストレージを使用できるようにするために、vSphere 管理者は、さまざまなストレージ要件とサービス クラスを記述するストレージ ポリシーを作成します。続いて、管理者は名前空間レベルでストレージ ポリシーを割り当てて、ストレージ制限を構成します。

vSphere IaaS control plane とパーシステント ストレージがどのように連携するかを理解するには、ストレージ クラス、パーシステント ボリューム、パーシステント ボリュームの要求など、Kubernetes の重要な概念を把握しておく必要があります。詳細については、Kubernetes のドキュメント (https://kubernetes.io/docs/home/) を参照してください。

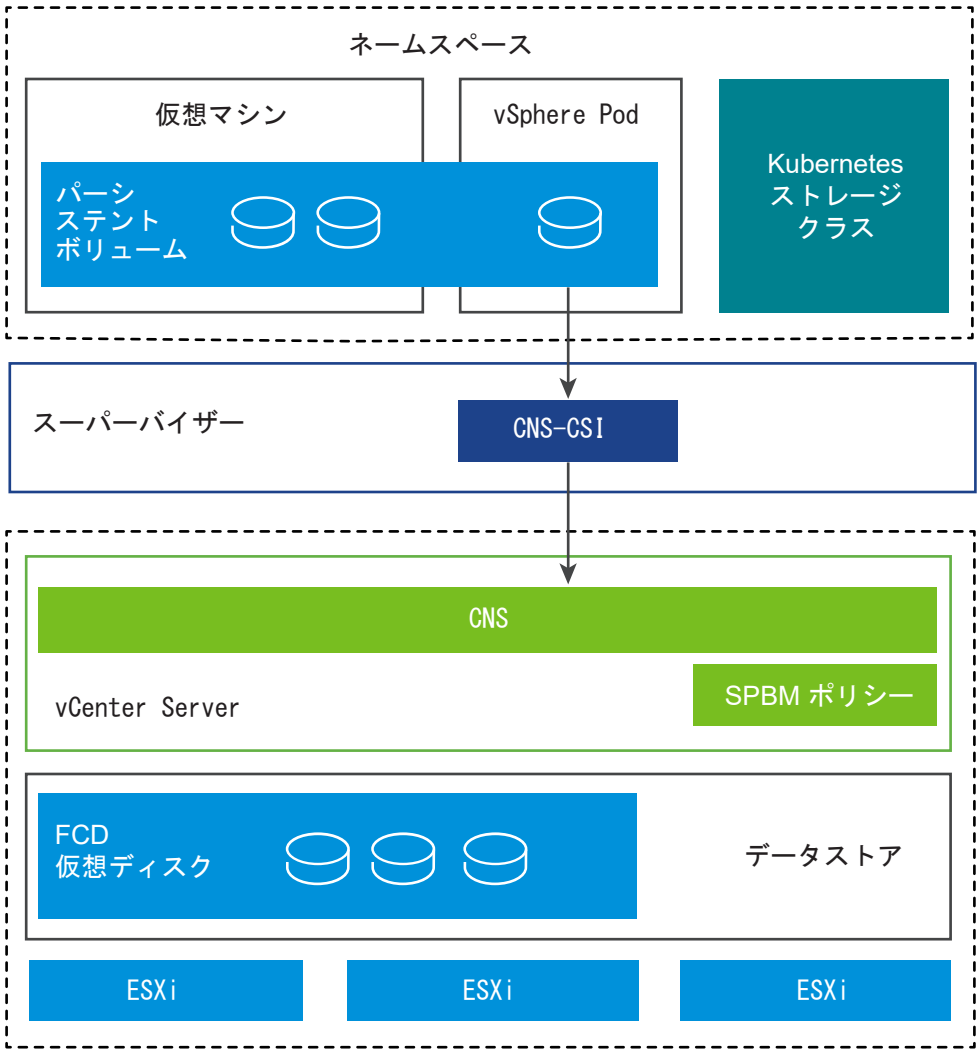
Tanzu Kubernetes Grid クラスタのパーシステント ストレージの詳細については、Tanzu Kubernetes Grid クラスタのストレージを参照してください。

パーシステント ストレージの使用方法については、『vSphere IaaS 制御プレーンのサービスとワークロード』ドキュメントのワークロードでのパーシステント ストレージの使用を参照してください。

DevOps チームがパーシステント ストレージのニーズに対して vSAN Direct を使用するサードパーティ サービスをデプロイする予定の場合は、『vSphere IaaS 制御プレーンのサービスとワークロード』ドキュメントの vSphere with Taznu でのステートフル サービスの有効化を参照してください。

スーパーバイザー と vSphere ストレージの統合方法

スーパーバイザー はいくつかのコンポーネントを使用して、vSphere ストレージと統合します。



vCenter Server 上のクラウド ネイティブ ストレージ (CNS)

CNS コンポーネントは、vCenter Server に配置されます。これは、パーシステント ボリュームのプロビジョニングとライフサイクルの操作を実装する vCenter Server 管理の拡張機能です。

パーシステント ボリュームをプロビジョニングするときに、コンポーネントは vSphere の最初のクラス ディスク機能と通信して、ボリュームをバッキングする仮想ディスクを作成します。また、CNS サーバ コンポーネントは、ストレージ ポリシーベースの管理と通信して、ディスクに必要なサービス レベルを確保します。

CNS は、vSphere 管理者が vCenter Server を介してパーシステント ボリュームとそのバッキング ストレージ オブジェクトを管理および監視するクエリ処理も実行します。

最初のクラス ディスク (FCD)

強化された仮想ディスクとも呼ばれます。これらのディスクはデータストアに配置され、ReadWriteOnce パーシステント ボリュームをバッキングします。

FCD を使用する場合は、次の点に注意してください。

- FCD は NFS 4.x プロトコルをサポートしません。代わりに、NFS 3 を使用してください。
- vCenter Server は、同じ FCD での操作をシリアル化しません。したがって、アプリケーションは同じ FCD で複数の操作を同時に実行できません。複数のスレッドからクローン作成、再配置、削除、取得などの操作を同時に実行すると、予期しない結果になります。問題を回避するには、アプリケーションが同じ FCD で操作を実行するときに、順番に実行する必要があります。
- FCD は管理対象オブジェクトではなく、単一 FCD への複数の書き込みから保護するグローバル ロックをサポートしていません。したがって、複数の vCenter Server インスタンスで同じ FCD を管理することはできません。FCD で複数の vCenter Server インスタンスを使用する必要がある場合は、次の方法を使用できます。
  - 複数の vCenter Server インスタンスで複数のデータストアを管理できます。
  - 複数の vCenter Server インスタンスが同じ FCD で動作することはありません。

ストレージ ポリシー ベースの管理

ストレージ ポリシー ベースの管理は、ストレージ ポリシーに記述されているストレージ要件に従って、パーシステント ボリュームとそのバッキング仮想ディスクのプロビジョニングをサポートする、vCenter Server サービスです。プロビジョニング後、サービスは、ストレージ ポリシー特性に対するボリュームのコンプライアンスを監視します。ストレージ ポリシーの管理の詳細については、『vSphere のストレージ』ドキュメントのストレージ ポリシー ベースの管理の章を参照してください。

vSphere CNS-CSI

vSphere CNS-CSI コンポーネントは、コンテナ ストレージ インターフェイス (CSI) 仕様に準拠しています。これは、Kubernetes のようなコンテナ オーケストレータによってパーシステント ストレージのプロビジョニングに使用されるインターフェイスを提供するために設計された業界標準です。CNS-CSI ドライバは スーパーバイザー で実行され、vSphere ストレージをある名前空間の Kubernetes 環境に接続します。vSphere CNS-CSI は、その名前空間から発生するすべてのストレージ プロビジョニング要求について、CNS コンポーネントと直接通信します。

vSphere CNS-CSI でサポートされる機能

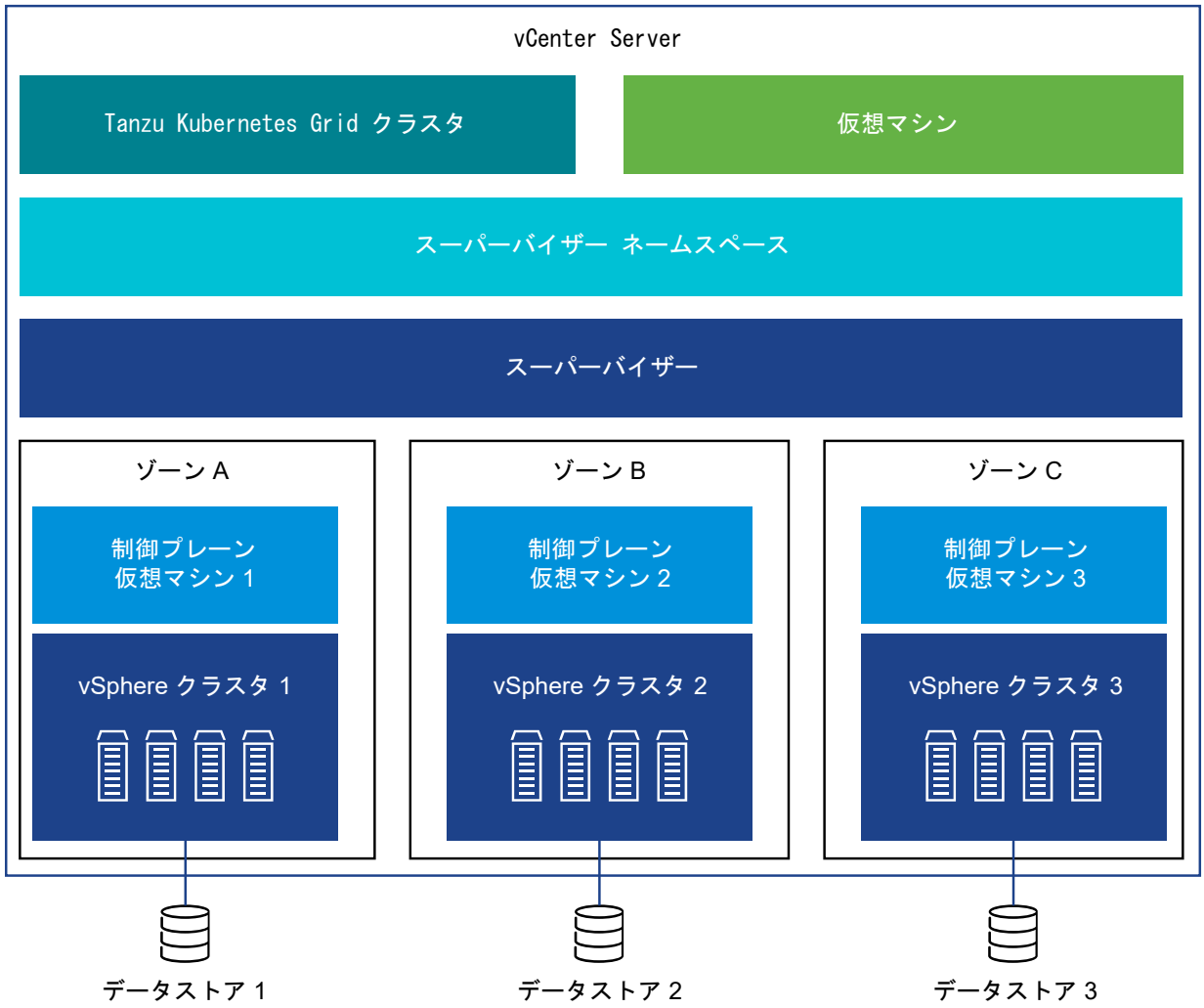
スーパーバイザー で実行される vSphere CNS-CSI コンポーネントは、複数の vSphere および Kubernetes ストレージ機能をサポートします。ただし、特定の制限が適用されます。

サポートされている機能	vSphere CNS-CSI と スーパーバイザー の併用
vSphere Client での CNS のサポート	はい
vSphere Client でのオブジェクト健全性の向上	はい（vSAN のみ）
動的ブロック パーシステント ボリューム（ReadWriteOnce アクセス モード）	はい
動的ファイル パーシステント ボリューム（ReadWriteMany アクセス モード）	いいえ
vSphere データストア	VMFS、NFS、vSAN（vSAN ESA を含む）、vVols
静的パーシステント ボリューム	はい

サポートされている機能	vSphere CNS-CSI と スーパーバイザー の併用
暗号化	いいえ
オフライン ボリュームの拡張	はい
オンライン ボリュームの拡張	はい
ボリューム トポロジとゾーン	はい。ボリュームは、Tanzu Kubernetes Grid クラスタでのみ使用できます。
Kubernetes の複数の制御プレーン インスタンス	はい
WaitForFirstConsumer	いいえ
VolumeHealth	はい
パーシステント ボリュームでの Storage vMotion	いいえ

vSphere Zone を使用したパーシステント ストレージと スーパーバイザー

3 ゾーン スーパーバイザー は、1 つのゾーン内のすべてのホスト間でデータストアが共有されるゾーン ストレージをサポートしています。



3 ゾーン スーパーバイザー にストレージ リソースを準備する場合は、次の考慮事項に注意してください。

- 3 つすべてのゾーン内のストレージが同じタイプである必要はありません。ただし、3 つすべてのクラスタで同じタイプのストレージを使用すると、一貫したパフォーマンスが得られます。
- 3 ゾーン スーパーバイザー の名前空間には、各クラスタの共有ストレージに準拠したストレージ ポリシーを使用します。ストレージ ポリシーはトポロジ対応である必要があります。
- 名前空間に割り当てた後は、ストレージ ポリシーからトポロジの制約を削除しないでください。
- ゾーン データストアを他のゾーンにマウントしないでください。
- 3 ゾーン スーパーバイザー では、次のアイテムはサポートされません。
  - ゾーン間ボリューム
  - vSAN ファイル ボリューム (ReadWriteMany ボリューム)
  - ボリューム登録 API を使用した静的ボリュームのプロビジョニング
  - vSAN データ パーシステンス プラットフォームを使用するワークロード
  - vSphere ポッド
  - vSAN ストレッチ クラスタ
  - vGPU とインスタンス ストレージを使用する仮想マシン

詳細については、『vSphere IaaS 制御プレーンのサービスとワークロード』ドキュメントの 3 ゾーン スーパーバイザーでのパーシステント ストレージの使用を参照してください。

Tanzu Kubernetes Grid アーキテクチャおよびコンポーネント

3

Tanzu Kubernetes Grid のアーキテクチャと、スーパーバイザーおよびそのコンポーネントとの統合方法を確認します。また、Tanzu Kubernetes Grid クラスタのネットワークとストレージの仕組み、および Tanzu Kubernetes Grid の高可用性とそれをサポートするスーパーバイザーのデプロイについても説明します。

次のトピックを参照してください。

- Tanzu Kubernetes Grid アーキテクチャ
- Tanzu Kubernetes Grid クラスタ ネットワーク
- Tanzu Kubernetes Grid クラスタのストレージ
- Tanzu Kubernetes Grid クラスタの高可用性
- Tanzu Kubernetes Grid 認証

Tanzu Kubernetes Grid アーキテクチャ

Tanzu Kubernetes Grid により、Tanzu Kubernetes Grid クラスタのライフサイクルをセルフサービスで管理できるようになります。Tanzu Kubernetes Grid を使用して Tanzu Kubernetes Grid クラスタを作成して管理する際は、Kubernetes のオペレータや開発者になじみのある、宣言による方法を使用します。

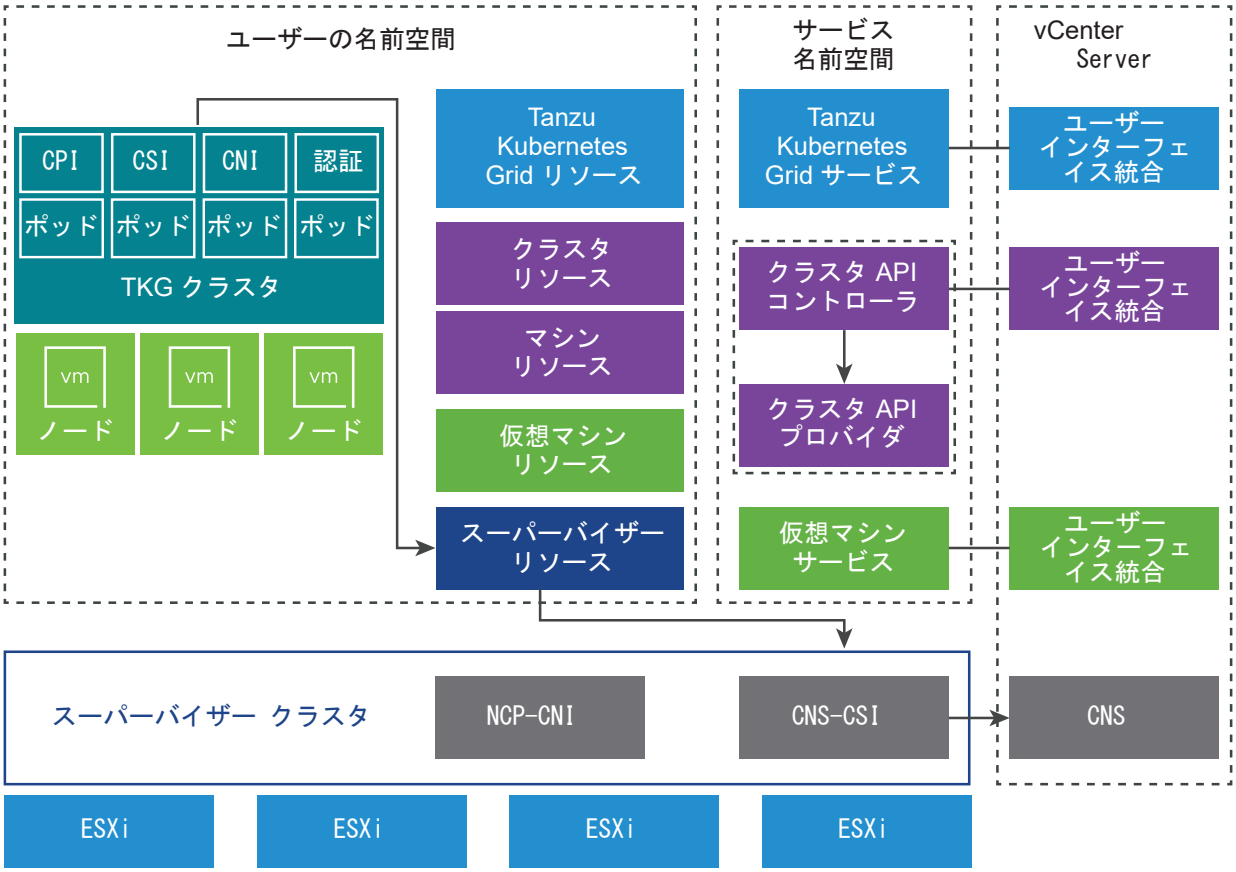
Tanzu Kubernetes Grid コンポーネント

Tanzu Kubernetes Grid は、Tanzu Kubernetes Grid クラスタのライフサイクルを管理するためにコントローラの 3 つのレイヤーを公開します。

- Tanzu Kubernetes Grid は、基盤となる vSphere 名前空間 リソースと統合するために必要なコンポーネントを含むクラスタをプロビジョニングします。これらのコンポーネントには、スーパーバイザー と連携するクラウド プロバイダ プラグインが含まれています。さらに、Tanzu Kubernetes Grid クラスタは、VMware クラウド ネイティブ ストレージ (CNS) と統合されている スーパーバイザー にパーシステント ボリュームの要求を渡します。ワークロードのパーシステント ストレージを参照してください。
- クラスタ API は、クラスタを作成、設定、および管理するための、宣言型の Kubernetes 形式 API を提供します。クラスタ API への入力には、クラスタを記述するリソース、クラスタを構成する仮想マシンを記述するリソースのセット、クラスタのアドオンを記述するリソースのセットなどがあります。

- 仮想マシン サービス は、仮想マシンとそれに関連する vSphere リソースを管理するための、宣言型の Kubernetes 形式 API を提供します。仮想マシン サービス により、抽象的な再利用可能ハードウェア構成を表す仮想マシン クラスの概念が導入されます。仮想マシン サービス の機能を使用すると、Tanzu Kubernetes Grid クラスタをホストする制御プレーンおよびワーカー ノード仮想マシンのライフサイクルを管理できます。

図 3-1. Tanzu Kubernetes Grid アーキテクチャおよびコンポーネント



Tanzu Kubernetes Grid クラスタ コンポーネント

Tanzu Kubernetes Grid クラスタで実行されるコンポーネントは、認証と認可、ストレージ統合、ポッド ネットワーク、ロード バランシングの 4 つの領域にわたっています。

- 認証 Webhook：クラスタ内のポッドとして動作し、ユーザー認証トークンを検証する Webhook。
- コンテナ ストレージ インターフェイス プラグイン：スーパーバイザー を介して CNS と統合される準仮想化 CSI プラグイン。
- コンテナ ネットワーク インターフェイス プラグイン：ポッド ネットワークを提供する CNI プラグイン。
- クラウド プロバイダの実装：Kubernetes ロード バランサ サービスの作成をサポートします。

Tanzu Kubernetes Grid API

Tanzu Kubernetes Grid クラスタをプロビジョニングおよび管理するには、Tanzu Kubernetes Grid API を使用します。これは、kubectl と YAML を使用して呼び出す宣言型 API です。VMware 拡張 kubectl 実行ファイルは、スーパーバイザー API エンドポイントの IP アドレスからダウンロードできます。

宣言型 API では、システムに対して命令型のコマンドを実行するのではなく、Tanzu Kubernetes Grid クラスタが達成する目的の状態を指定します。具体的には、ノードの数、使用可能なストレージ、仮想マシンのサイズ、Kubernetes ソフトウェアのバージョンを指定します。Tanzu Kubernetes Grid は、目的の状態を満たすクラスタをプロビジョニングするための作業を実行します。

Tanzu Kubernetes Grid API を呼び出すには、YAML ファイルを使用して kubectl を呼び出します。これによって API が呼び出されます。クラスタが作成されたら、YAML を更新してクラスタを更新します。

Tanzu Kubernetes Grid クラスタ ネットワーク

Tanzu Kubernetes Grid によってプロビジョニングされた Tanzu Kubernetes Grid クラスタでは、Antrea（デフォルト）と Calico の 2 つの CNI オプションがサポートされています。いずれも、クラスタのポッド、サービス、および Ingress 用のネットワークを提供するオープンソース ソフトウェアです。

Tanzu Kubernetes Grid によってプロビジョニングされた Tanzu Kubernetes Grid クラスタでは、次の コンテナ ネットワーク インターフェイス (CNI) オプションがサポートされます。

- Antrea
- Calico

Antrea は、新しい Tanzu Kubernetes Grid クラスタのデフォルトの CNI です。Antrea を使用する場合、クラスタのプロビジョニング中に CNI として指定する必要はありません。Calico を CNI として使用するには、次の 2 つの方法があります。

- クラスタの YAML で直接 CNI を指定します。v1alpha3 の例：カスタム ネットワークを使用する TKC を参照してください。
- デフォルトの CNI を変更します。v1beta1 の例：Calico CNI を含むクラスタを参照してください。

注： Antrea をデフォルトの CNI として使用するには、Tanzu Kubernetes Grid クラスタ用の OVA ファイルの最小バージョンが必要です。スーパーバイザーでの TKG 2 クラスタのアップデートを参照してください。

次の表に、Tanzu Kubernetes Grid クラスタのネットワーク機能とその実装の概要を示します。

表 3-1. Tanzu Kubernetes Grid クラスタ ネットワーク

エンドポイント	プロバイダ	説明
ポッドの接続	Antrea または Calico	ポッドのコンテナ ネットワーク インターフェイス。Antrea は Open vSwitch を使用します。Calico は BGP を利用する Linux ブリッジを使用します。
サービス タイプ：ClusterIP	Antrea または Calico	クラスタ内からのみアクセス可能なデフォルトの Kubernetes サービス タイプ。

表 3-1. Tanzu Kubernetes Grid クラスタ ネットワーク （続き）

エンドポイント	プロバイダ	説明
サービス タイプ：NodePort	Antrea または Calico	Kubernetes ネットワーク プロキシによって各ワーカー ノードで開かれているポートを介して外部からアクセスできるようにします。
サービス タイプ：LoadBalancer	NSX-T ロード バランサ、NSX Advanced Load Balancer、HAProxy	NSX-T では、サービス タイプの定義ごとに 1 台の仮想サーバ。NSX Advanced Load Balancer については、このドキュメントの該当するセクションを参照してください。 **注：** 固定 IP アドレスのサポートなどの一部のロード バランシング機能は、HAProxy で使用できない場合があります。
クラスタの Ingress	サードパーティ製の Ingress コントローラ	受信ポッド トラフィックのルーティング。Contour などの任意のサードパーティ製 Ingress コントローラを使用できます。
ネットワーク ポリシー	Antrea または Calico	選択したポッドとネットワーク エンドポイントの間で送受信されるトラフィックを制御します。Antrea は Open vSwitch を使用します。Calico は Linux IP テーブルを使用します。

Tanzu Kubernetes Grid クラスタのストレージ

Tanzu Kubernetes Grid クラスタには、スーパーバイザー 名前空間で実行されるその他のコンポーネントおよびワークロードとして、パーシステント ストレージが必要です。

Tanzu Kubernetes Grid クラスタのストレージ ポリシー

Tanzu Kubernetes Grid クラスタにパーシステント ストレージ リソースを提供するために、vSphere 管理者は、さまざまなストレージ要件を記述するストレージ ポリシーを構成します。次に、そのストレージ ポリシーを、Tanzu Kubernetes Grid クラスタがデプロイされている名前空間に追加します。名前空間で認識されるストレージ ポリシーにより、名前空間がどのデータストアにアクセスしてパーシステント ストレージに使用できるかが決まります。ストレージ ポリシーでは、vSphere ストレージ環境でのクラスタ ノードとワークロードの配置方法が指示されます。

名前空間に割り当てられたストレージ ポリシーに基づいて、vSphere IaaS control plane によって、名前空間に自動的に表示される、対応する Kubernetes ストレージ クラスが作成されます。このストレージ クラスは、この名前空間の Tanzu Kubernetes Grid クラスタにも伝達されます。

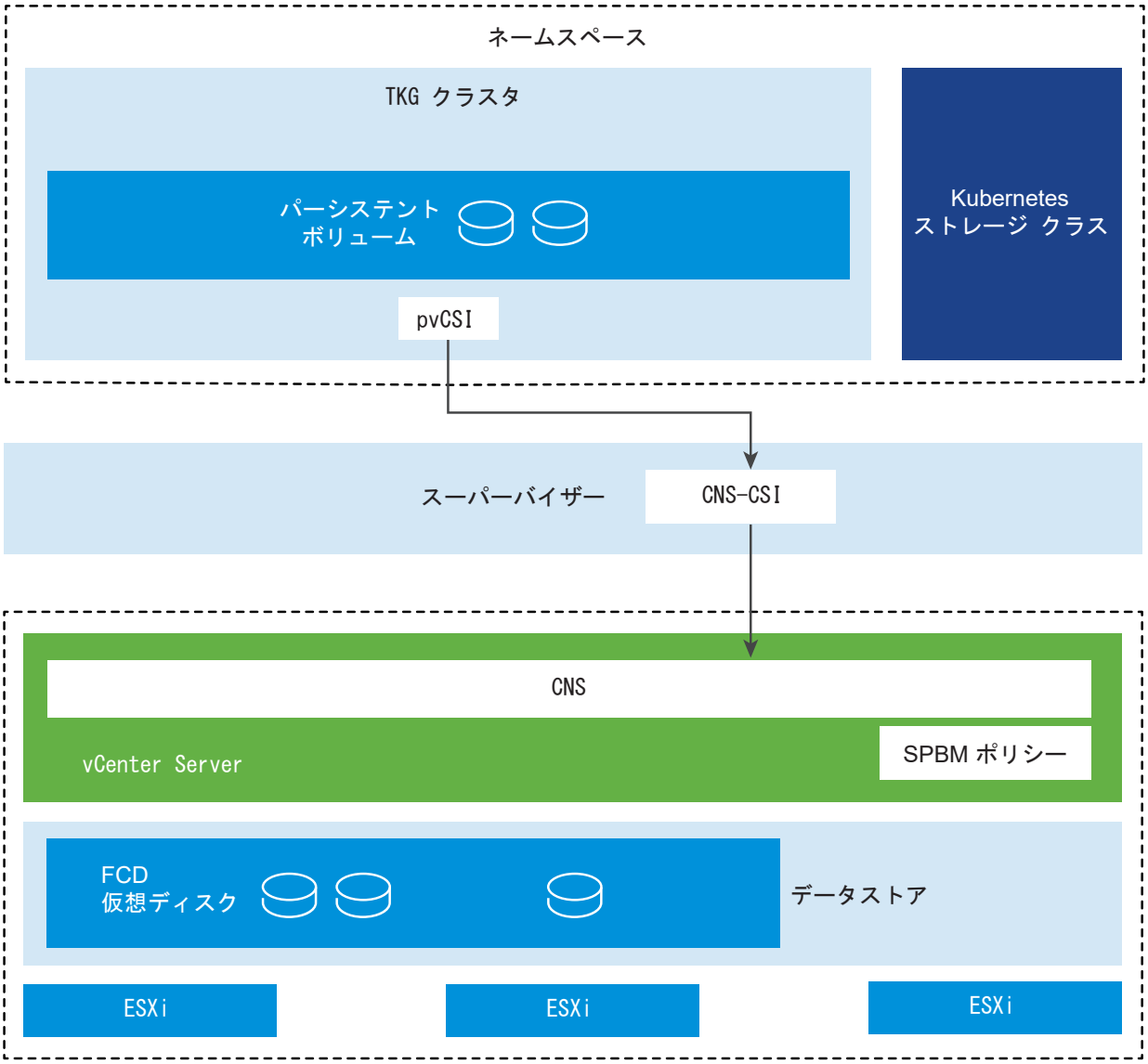
Tanzu Kubernetes Grid クラスタでは、このストレージ クラスが 2 つのエディション（`Immediate` および `WaitForFirstConsumer` バインド モード）に表示されます。DevOps チームが選択するエディションは要件によって異なります。

Tanzu Kubernetes Grid クラスタのストレージ クラスの詳細については、パーシステント ボリュームのためのストレート クラスの使用を参照してください。

Tanzu Kubernetes Grid クラスタと vSphere ストレージの統合方法

スーパーバイザー と vSphere ストレージを統合するために、Tanzu Kubernetes Grid クラスタでは準仮想化 CSI (pvCSI) が使用されます。

pvCSI は Tanzu Kubernetes Grid クラスタ用に変更された vSphere CNS-CSI ドライバのバージョンです。pvCSI は Tanzu Kubernetes Grid クラスタに配置され、Tanzu Kubernetes Grid クラスタから送信されるすべてのストレージ関連の要求に対処します。要求は CNS-CSI に配信され、vCenter Server の CNS に伝達されます。その結果、pvCSI は CNS コンポーネントとの直接通信は行わず、すべてのストレージ プロビジョニング操作に CNS-CSI を使用します。CNS-CSI とは異なり、pvCSI はインフラストラクチャの認証情報を必要としません。名前空間のサービス アカウントを使用して構成されます。

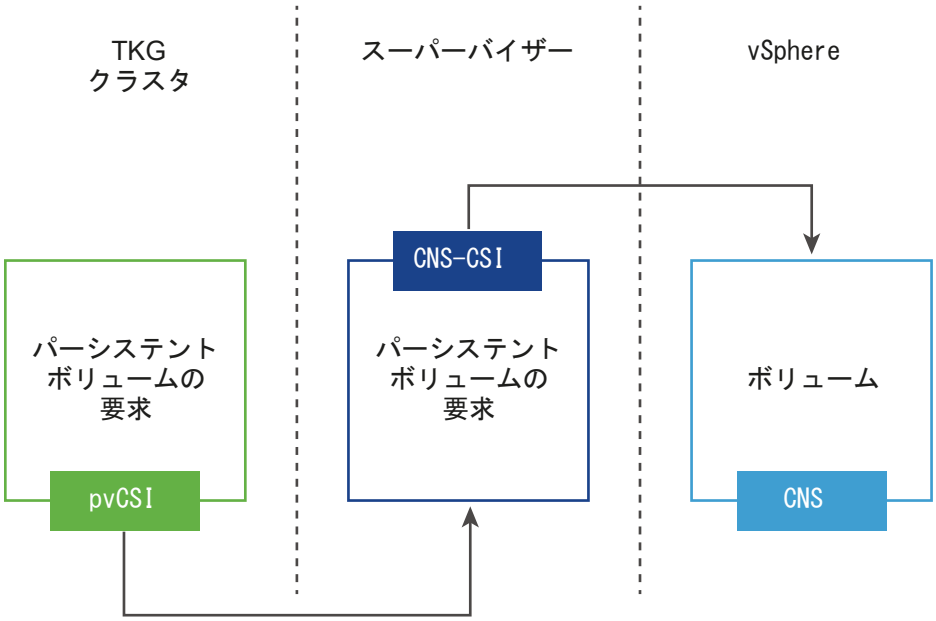


vSphere ストレージとの統合に使用される スーパーバイザー コンポーネントの詳細については、ワークロードのパーシステント ストレージを参照してください。

パーシステント ボリュームの作成方法

次の図は、DevOps エンジニアが Tanzu Kubernetes Grid クラスタ内でストレージ関連の操作（たとえば、パーシステント ボリューム要求 (PVC) の作成）を実行するときに、さまざまなコンポーネントがどのように相互作用するかを示しています。

DevOps エンジニアは、Tanzu Kubernetes Grid クラスタでコマンド ラインを使用して PVC を作成します。このアクションにより、対応する PVC が スーパーバイザー に生成され、CNS-CSI がトリガされます。CNS-CSI は、CNS ボリューム作成 API を呼び出します。



ボリュームの作成が正常に完了すると、操作は スーパーバイザー を介して元の Tanzu Kubernetes Grid クラスタに伝達されます。この伝達の結果、ユーザーは、スーパーバイザー でバインド状態のパーシステント ボリュームとパーシステント ボリュームの要求を確認できます。また、バインド状態のパーシステント ボリュームとパーシステント ボリュームの要求は Tanzu Kubernetes Grid クラスタでも確認できます。

pvCSI でサポートされる機能

Tanzu Kubernetes Grid クラスタで実行される pvCSI コンポーネントでは、多くの vSphere および Kubernetes のストレージ機能がサポートされています。

サポートされている機能	pvCSI と Tanzu Kubernetes Grid クラスタの併用
vSphere Client での CNS のサポート	はい
vSphere Client でのオブジェクト健全性の向上	はい（vSAN のみ）
動的ブロック パーシステント ボリューム（ReadWriteOnce アクセス モード）	はい
動的ファイル パーシステント ボリューム（ReadWriteMany アクセス モード）	はい（vSAN ファイル サービスを使用）
vSphere データストア	VMFS/NFS/vSAN/vVols
静的パーシステント ボリューム	はい
暗号化	いいえ

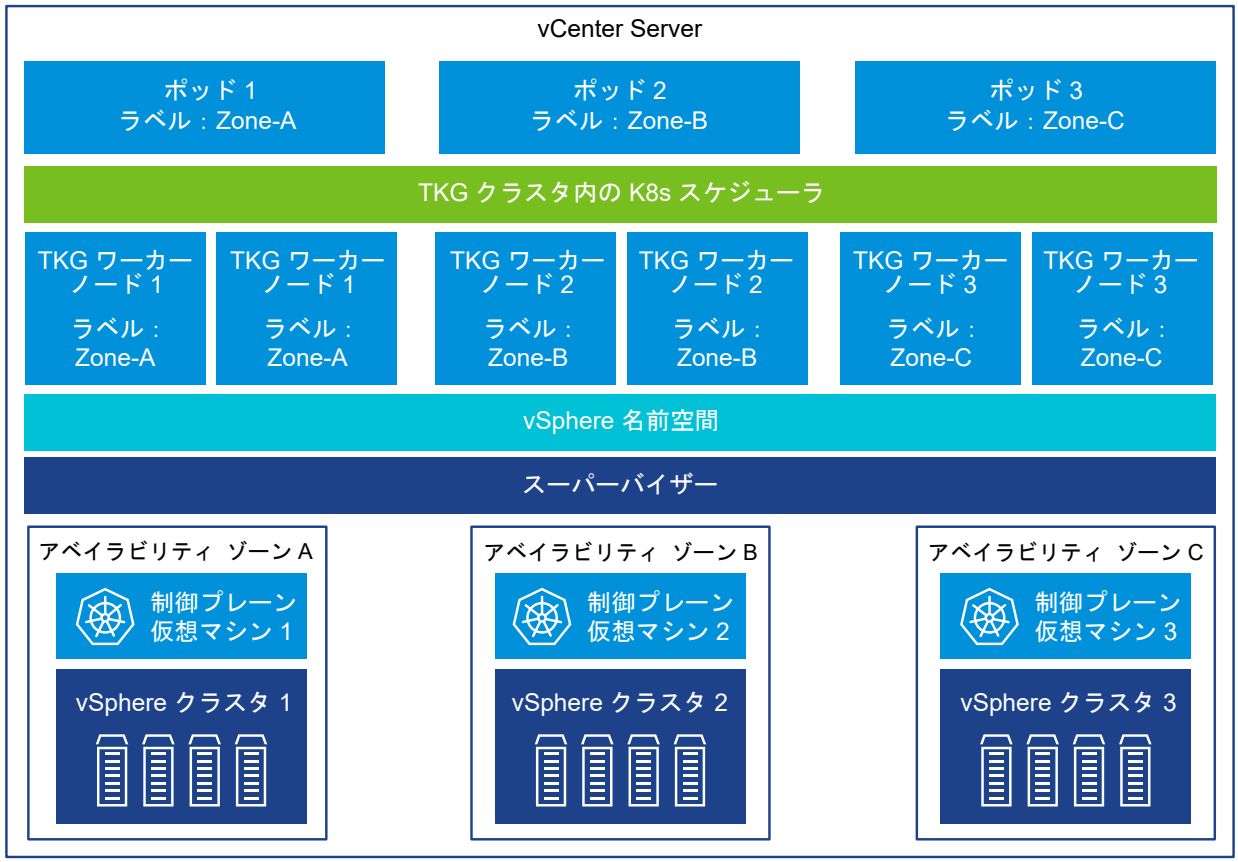
サポートされている機能	pvCSI と Tanzu Kubernetes Grid クラスタの併用
オフライン ボリュームの拡張	はい
オンライン ボリュームの拡張	はい
ボリューム トポロジとゾーン	はい
Kubernetes の複数の制御プレーン インスタンス	はい
WaitForFirstConsumer	はい
VolumeHealth	はい
パーシステント ボリュームでの Storage vMotion	いいえ

Tanzu Kubernetes Grid クラスタの高可用性

3 つの vSphere Zone スーパーバイザー にデプロイされている Tanzu Kubernetes Grid クラスタに可用性を提供することができます。vSphere Zone は vSphere クラスタにマッピングされます。つまり、スーパーバイザー を 3 つの vSphere Zone にデプロイすると、基盤となる 3 つすべての vSphere クラスタのリソースが使用されます。これにより、Tanzu Kubernetes Grid クラスタ内で実行中の Kubernetes ワークロードが、vSphere クラスタ レベルの障害から保護されます。単一ゾーン デプロイでは、Tanzu Kubernetes Grid クラスタの高可用性は、vSphere HA によって ESXi ホスト レベルで提供されます。

3 ゾーン スーパーバイザー では、Tanzu Kubernetes Grid クラスタの制御プレーン ノードは自動的に vSphere Zone 間に配置されます。ただし、ワーク ノードがゾーン間で分散される方法を制御できます。Tanzu Kubernetes Grid クラスタのワーカー ノードに対し NodePool オブジェクトを定義し、各 vSphere Zone を各 NodePool 内の FailureDomain にマッピングできます。このように、クラスタ API によってワーカー ノードが適宜に vSphere Zone 間で分散されます。1 つまたはすべての NodePool に対する FailureDomain の指定をスキップすると、クラスタ API によって NodePool がゾーン間で自動的に分散されます。

図 3-2. 複数のゾーンに配置された Tanzu Kubernetes Grid クラスタの高可用性



Tanzu Kubernetes Grid 認証

さまざまな認証メカニズムと Tanzu Kubernetes Grid クラスタでのそれらの使用方法について説明します。

スーパーバイザーへの接続

DevOps エンジニアは、スーパーバイザーを接続して Tanzu Kubernetes Grid クラスタをプロビジョニングします。vSphere 管理者によって権限が設定された名前空間にのみアクセスできます。

Kubernetes 制御プレーンの IP アドレスのスーパーバイザーまたはプロビジョニングされた Tanzu Kubernetes Grid クラスタに接続するには、次の 2 つの方法のどちらかを使用します。

- vCenter Single Sign-On と vSphere 向け Kubernetes CLI Tools。この場合、10 時間ごとに有効期限が切れる認証トークンが作成されます。
- スーパーバイザーと Tanzu CLI に登録された OIDC プロバイダから取得する認証情報。OIDC プロバイダとのセッションは、プロバイダ自体の設定によって制御されます。

詳細については、『vSphere IaaS 制御プレーンでの TKG サービスの使用』を参照してください。

Tanzu Kubernetes Grid クラスタへの接続

DevOps エンジニアは、プロビジョニングされた Tanzu Kubernetes Grid クラスタにも接続して、それらを運用および管理します。Tanzu Kubernetes Grid クラスタがプロビジョニングされている vSphere 名前空間に対する編集権限がユーザー アカウントに付与されると、そのアカウントが `cluster-admin` ロールに割り当てられます。または、`kubernetes-admin` ユーザーを使用して、Tanzu Kubernetes Grid クラスタに接続することもできます。ユーザーまたはグループをデフォルトまたはカスタムのポッド セキュリティ ポリシーにバインドすることにより、開発者に Tanzu Kubernetes Grid クラスタへのアクセス権を付与することもできます。詳細については、『vSphere IaaS 制御プレーンでの TKG サービスの使用』を参照してください。

スーパーバイザー デプロイのオプション

4

スーパーバイザー をデプロイおよび構成するためのオプションを確認します。スーパーバイザー 用に実装するネットワーク スタックまたはデプロイ オプションに応じて、サポートされるトポロジとワークロード タイプは異なります。

次のトピックを参照してください。

- スーパーバイザー ゾーンおよびクラスタのデプロイ
- Distributed Switch ネットワークと NSX Advanced Load Balancer を使用した スーパーバイザー のトポロジ
- NSX をネットワーク スタックとして使用する単一ゾーンの スーパーバイザー のトポロジ
- NSX（ネットワーク スタックとして）と NSX Advanced Load Balancer を使用する単一ゾーンの スーパーバイザー のトポロジ
- HAProxy ロード バランサをデプロイするトポロジ

スーパーバイザー ゾーンおよびクラスタのデプロイ

複数の vSphere Zone にマッピングされる 3 つの vSphere クラスタに スーパーバイザー をデプロイする場合と、1 つの vSphere Zone にマッピングされる スーパーバイザー の単一クラスタのデプロイの違いについて説明します。

注： 単一の vSphere クラスタに スーパーバイザー をデプロイすると、1 つの vSphere Zone が作成されるため、スーパーバイザー を 3 ゾーンのデプロイに拡張することはできません。1 つの vSphere Zone（単一クラスタのデプロイ）または 3 つの vSphere Zone に スーパーバイザー をデプロイできます。

クラスタレベルの HA のための スーパーバイザー の 3 ゾーンのデプロイ

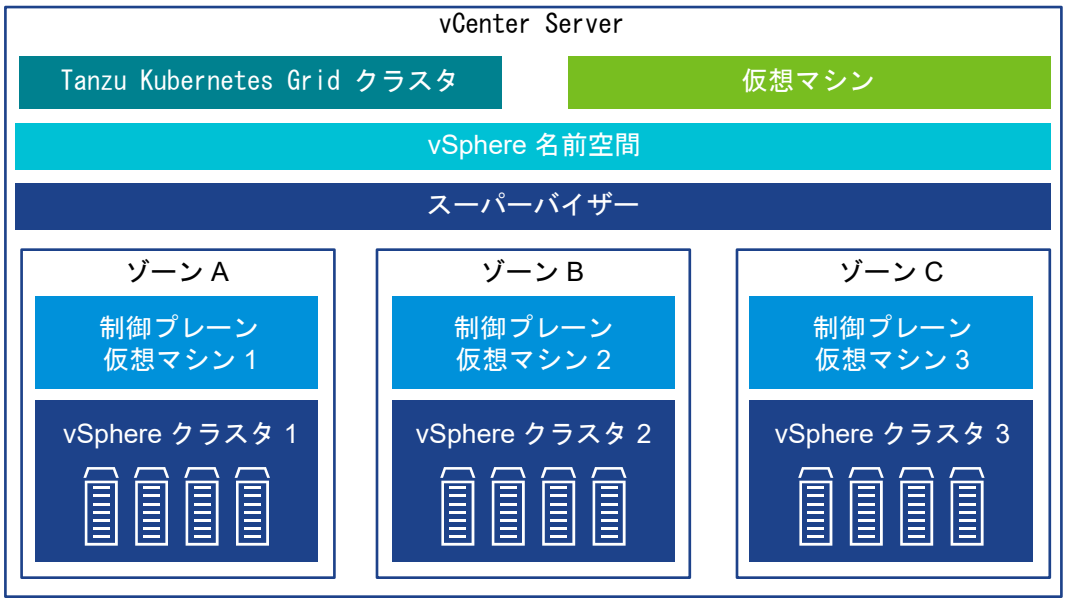
3 つの vSphere Zone にマッピングされる 3 つの vSphere クラスタで vSphere IaaS control plane を有効にすることができます。各 vSphere クラスタを独立した障害ドメインとして構成し、1 つの vSphere Zone にマッピングします。3 ゾーンのデプロイでは、3 つの vSphere クラスタがすべて 1 つの スーパーバイザー になります。3 ゾーンのデプロイでは、次のことが可能です。

- 各 vSphere クラスタは独立した障害ドメインであるため、クラスタレベルの高可用性を スーパーバイザー に提供します。

- 3 つのすべての vSphere Zone に Tanzu Kubernetes Grid クラスタのノードを分散し、vSphere クラスタ レベルで Kubernetes ワークロードに HA を提供します。
- 3 つの各 vSphere クラスタにホストを追加して スーパーバイザー を拡張します。

Tanzu Kubernetes Grid クラスタ、vSphere ポッド、仮想マシンを使用して、3 ゾーンのスーパーバイザーでワークロードを実行できます。

図 4-1. 3 ゾーンのスーパーバイザーのデプロイ



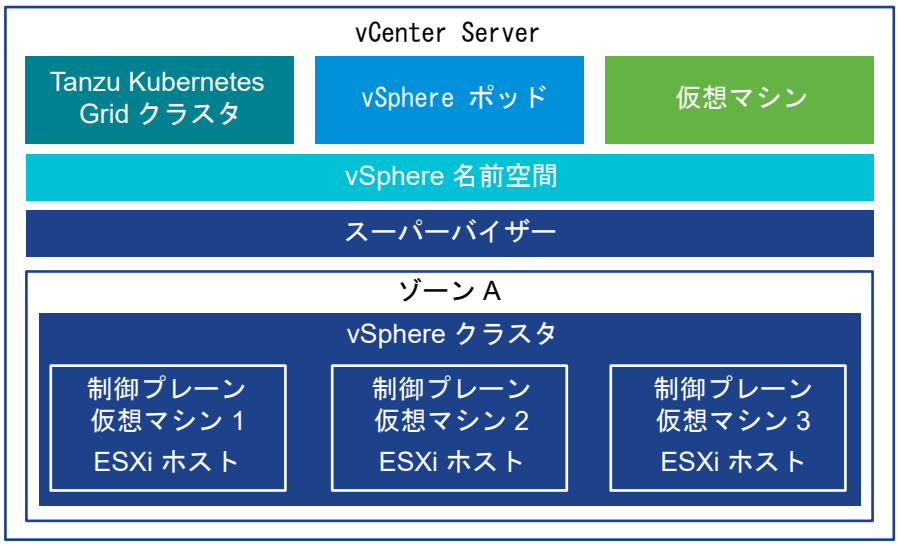
複数の物理サイトにまたがる vSphere ゾーンの配置

サイト間の遅延が 100 ミリ秒を超えない限り、vSphere ゾーンを複数の物理サイトに分散できます。たとえば、vSphere ゾーンを 2 つのサイトに配置する場合、一方のサイトに vSphere ゾーンを 1 つ、もう一方のサイトに 2 つ配置して分散させることができます。

スーパーバイザー の単一クラスタのデプロイ

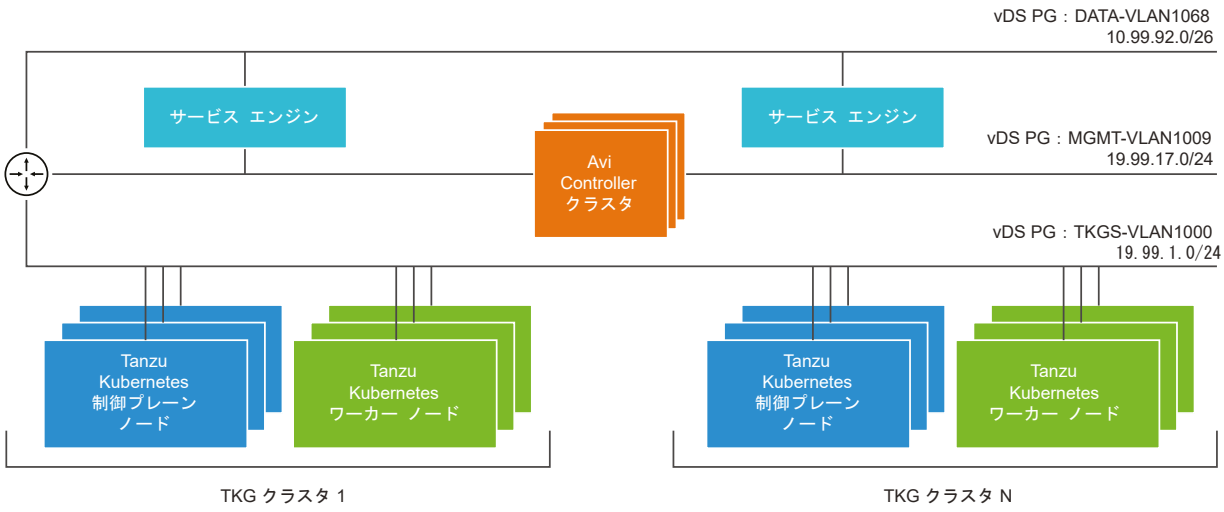
単一の vSphere クラスタでも スーパーバイザー を有効にすることができます。この場合、単一のゾーンが スーパーバイザー 用に自動的に作成されるか、事前に作成したゾーンを使用できます。単一クラスタのデプロイでは、vSphere HA を介したクラスタレベルの高可用性が確保されます。また、vSphere IaaS control plane のセットアップを拡張するには、スーパーバイザー にマッピングされる vSphere クラスタにホストを追加する必要があります。単一クラスタのデプロイでは、vSphere ポッド、Tanzu Kubernetes Grid クラスタ、および仮想マシン サービスを介してデプロイされた仮想マシンを使用してワークロードを実行できます。

図 4-2. 単一クラスタの スーパーバイザー のデプロイ



Distributed Switch ネットワークと NSX Advanced Load Balancer を使用した スーパーバイザー のトポロジ

Avi Controller は常に管理ネットワークにデプロイされ、vCenter Server、ESXi ホスト、および スーパーバイザー 制御プレーン ノードとのインターフェイスを行うことができます。サービス エンジンは、管理ネットワークおよびデータ ネットワークへのインターフェイスを使用してデプロイされます。



MGMT-VLAN1009 などの管理ネットワークには Avi Controller が配置され、サービスエンジンの管理インターフェイスが接続されます。

DATA-VLAN1068 などのデータ ネットワークには、仮想 IP アドレスを配置するためのサービス エンジン インターフェイスが接続されます。クライアント トラフィックが VIP に到達すると、サービス エンジンはこのネットワークを介してワークロード ネットワーク IP アドレスへのトラフィックをロード バランシングします。

TKGS-VLAN1000 などのワークロード ネットワークでは、Tanzu Kubernetes Grid クラスタが実行されます。サービス エンジンは、ワークロード ネットワークへのインターフェイスを必要としません。

サービス エンジンはワンアーム モードで実行されます。ロード バランシングされたトラフィックは、サービス エンジンによってルーター経由でワークロード ネットワークにルーティングされます。サービス エンジンは、データ ネットワークの DHCP からデフォルト ゲートウェイの IP アドレスを取得しません。サービス エンジンがワークロード ネットワークおよびクライアント IP アドレスにトラフィックを適切にルーティングできるように、スタティック ルートを構成する必要があります。

このトポロジでは、サービス エンジンを単一のネットワークに配置できます。サービス エンジンの作成とネットワーク接続は、Avi Controller によって自動実行されます。

NSX Advanced Load Balancer のインストールと構成の詳細については、NSX Advanced Load Balancer のインストールと構成を参照してください。

NSX Advanced Load Balancer コンポーネント

NSX Advanced Load Balancer（別名、Avi Load Balancer）のコンポーネントには、Controller クラスタ、サービス エンジン（データ プレーン）仮想マシン、Avi Kubernetes Operator (AKO) などがあります。

NSX Advanced Load Balancer コンポーネントのインストールと構成の詳細については、NSX Advanced Load Balancer のインストールと構成を参照してください。

コントローラ

NSX Advanced Load Balancer Controller（別名、コントローラ）は vCenter Server と連携して Tanzu Kubernetes Grid クラスタのロード バランシングを自動実行します。コントローラは、サービス エンジンのプロビジョニング、サービス エンジン間でのリソースの調整、サービス エンジンのメトリックとログの集計を行います。また、ユーザー操作およびプログラムによる連携のための Web インターフェイス、コマンドライン インターフェイス、および API を提供します。

vSphere でコントローラ仮想マシンをデプロイして構成した後、コントローラ クラスタをデプロイして、HA 用の制御プレーン クラスタを設定できます。

NSX Advanced Load Balancer がインストールされている、または動作している環境のコンテナとなるのはクラウドです。コントローラの初期構成時に、[Default-cloud] という名前のクラウドが自動的に作成されます。[Default-cloud] を [VMware vCenter] クラウドとして使用することも、[VMware vCenter] タイプのカスタム クラウドを 1 つ以上作成することもできます。

[VMware vCenter] タイプのクラウドを構成すると、固有の vCenter Server とその vCenter Server 内のデータセンターに関連付けられます。その vCenter Server およびデータセンターで使用可能なすべてのリソースを、クラウドで使用できます。

ロード バランサを複数の vCenter Server や複数のデータセンターに使用できるようにするには、[VMware vCenter] タイプのカスタム クラウドを、vCenter Server とデータセンターの組み合わせごとに 1 つ作成します。これにより、環境をサポートするために必要なロード バランサ インスタンスの数が減り、結果としてコア数も少なくなるため、運用上の負荷が軽減されます。クラウドの詳細については、NSX Advanced Load Balancer のドキュメントを参照してください。

サービス エンジン

サービス エンジンとも呼ばれる NSX Advanced Load Balancer サービス エンジンは、データ プレーン仮想マシンです。サービス エンジンは 1 つ以上の仮想サービスを実行します。サービス エンジンはコントローラによって管理されます。コントローラは、仮想サービスをホストするようにサービス エンジンをプロビジョニングします。

サービス エンジンには、次の 2 種類のネットワーク インターフェイスがあります。

- 仮想マシンの最初のネットワーク インターフェイス `vnic0` は管理ネットワークに接続され、そこから NSX Advanced Load Balancer Controller に接続することができます。
- もう一方のインターフェイス `vnic1 - 9` は、仮想サービスが実行されるワークロード ネットワークに接続されます。

サービス エンジン インターフェイスは、適切な Distributed Switch ポート グループに自動的に接続します。使用されていないインターフェイスは、切断状態の管理ネットワーク ポート グループに接続されます。各サービス エンジンは、最大 1,000 個の仮想サービスをサポートできます。

仮想サービスは、Tanzu Kubernetes Grid クラスタ ワークロード用のレイヤー 4 およびレイヤー 7 ロード バランシング サービスを提供します。仮想サービスは、1 つの仮想 IP アドレスと複数のポートで構成されます。仮想サービスをデプロイすると、コントローラによって ESX サーバが自動的に選択され、サービス エンジンが起動して適切なネットワーク（ポート グループ）に接続します。

最初のサービス エンジンは、最初の仮想サービスが構成された後にのみ作成されます。以降に構成された仮想サービスは、既存のサービス エンジンを使用します。

各仮想サーバは、Tanzu Kubernetes Grid クラスタのロード バランサ タイプの異なる IP アドレスを持つレイヤー 4 ロード バランサを公開します。各仮想サーバに割り当てられる IP アドレスは、構成時にコントローラに指定する IP アドレス ブロックから選択されます。

Avi には、ネイティブ IP アドレス管理と外部 IP アドレス管理プロバイダのサポートが付属しています。vSphere では、Avi のネイティブ IP アドレス管理が利用されます。

Avi Kubernetes オペレータ

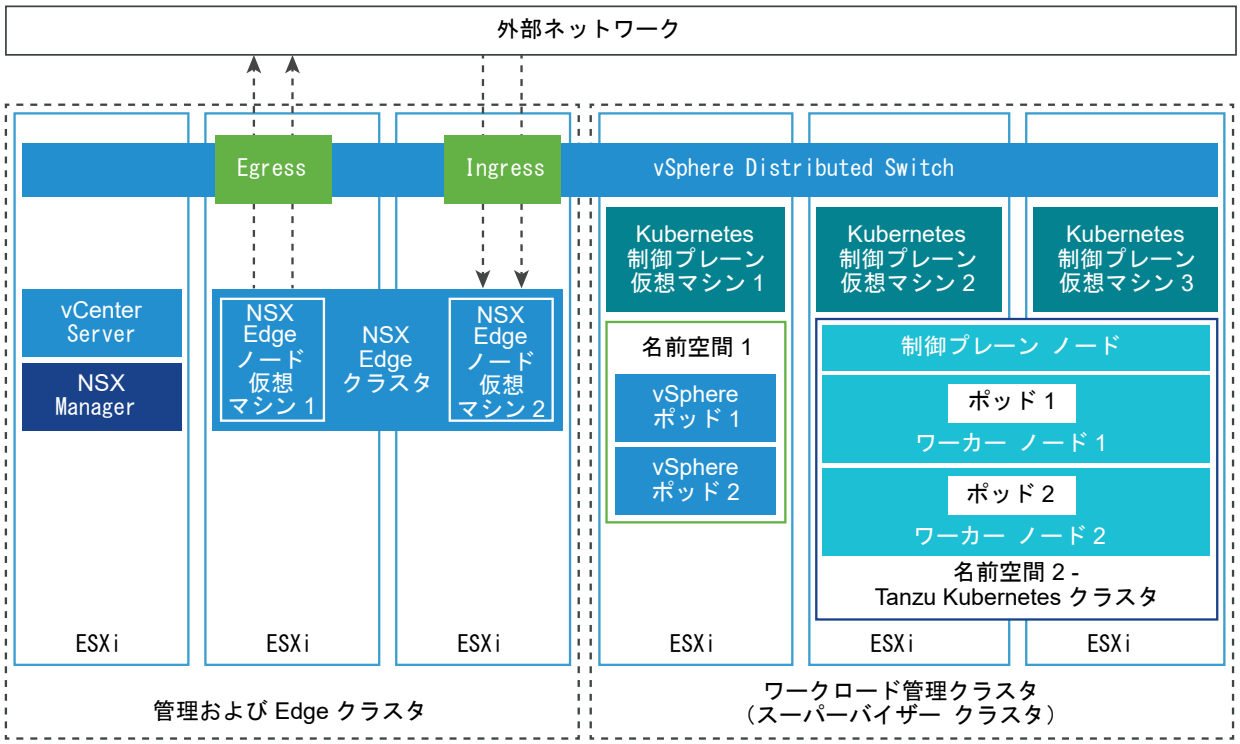
Avi Kubernetes Operator (AKO) は Kubernetes リソースを監視し、コントローラと通信して、対応するロード バランシング リソースを要求します。

Avi Kubernetes Operator は、有効化プロセスの一環として スーパーバイザー にインストールされます。

NSX をネットワーク スタックとして使用する単一ゾーンの スーパーバイザー のトポロジ

vSphere IaaS control plane は、2 つのクラスタにデプロイできます。1 つは管理機能と Edge 機能用、もう 1 つはワークロード管理専用です。

図 4-3. 管理および Edge クラスタとワークロード管理クラスタ



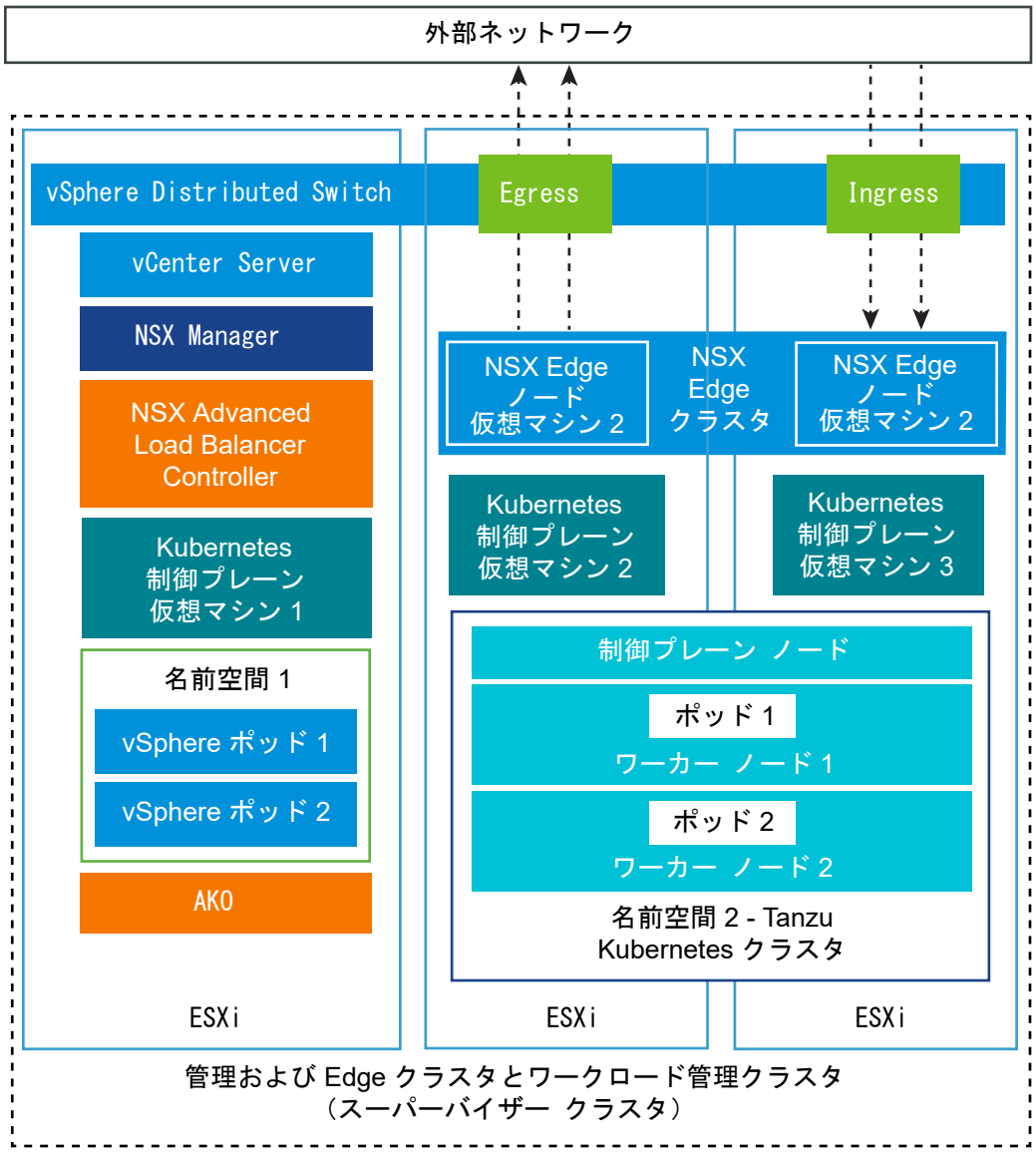
NSX（ネットワーク スタックとして）と NSX Advanced Load Balancer を使用する単一ゾーンの スーパーバイザー のトポロジ

Kubernetes ワークロードのニーズや基盤となるネットワーク インフラストラクチャに応じて、スーパーバイザーにさまざまなトポロジを適用できます。

管理、Edge、およびワークロード ドメイン クラスタのトポロジ

管理、Edge、およびワークロード管理の機能を 1 つの vSphere クラスタに統合した vSphere IaaS control plane をデプロイできます。

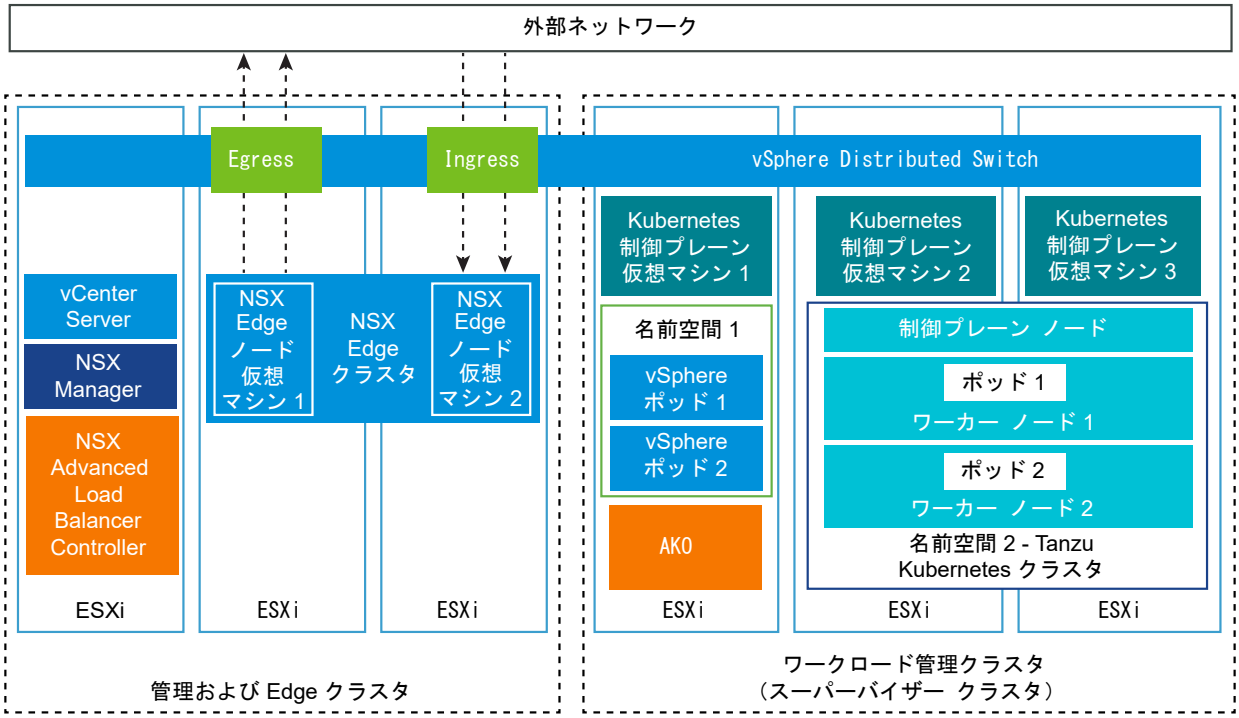
図 4-4. 管理、Edge、およびワークロード管理クラスタ



管理および Edge クラスタと、ワークロード管理クラスタを分離したトポロジ

vSphere IaaS control plane は、2 つのクラスタにデプロイできます。1 つは管理機能と Edge 機能用、もう 1 つはワークロード管理専用です。

図 4-5. 管理および Edge クラスタとワークロード管理クラスタ



HAProxy ロード バランサをデプロイするトポロジ

Distributed Switch ネットワークで構成された スーパーバイザー の HAProxy ロード バランサに実装可能なトポロジを確認します。vSphere IaaS control plane と Distributed Switch ネットワークを併用している場合、HAProxy は、Tanzu Kubernetes Grid 制御プレーンにアクセスする開発者と、ロード バランサ タイプの Kubernetes サービスに対応したロード バランシングを提供します。

スーパーバイザー のワークロード ネットワーク

Distributed Switch ネットワークを使用した スーパーバイザー を構成するには、クラスタ内のすべてのホストを Distributed Switch に接続する必要があります。スーパーバイザー ワークロード ネットワーク用に実装するトポロジに応じて、1 つ以上の分散ポート グループを作成します。作成したポート グループを、ワークロード ネットワークとして、vSphere 名前空間 に指定します。

ワークロード ネットワークは、Tanzu Kubernetes Grid クラスタのノードと、スーパーバイザー 制御プレーン仮想マシンへの接続を提供します。Kubernetes 制御プレーン仮想マシンに接続を提供するワークロード ネットワークは、プライマリ ワークロード ネットワークと呼ばれます。各 スーパーバイザー にそれぞれ 1 つのプライマリ ワークロード ネットワークが必要です。スーパーバイザー に対して、分散ポート グループの 1 つをプライマリ ワークロード ネットワークとして指定する必要があります。

注： ワークロード ネットワークが追加されるのは スーパーバイザー を有効にするときだけで、後で追加することはできません。

スーパーバイザー 上の Kubernetes 制御プレーン仮想マシンは、プライマリ ワークロード ネットワークに割り当てられた IP アドレス範囲から 3 つの IP アドレスを使用します。Tanzu Kubernetes Grid クラスタの各ノードには、この Tanzu Kubernetes Grid クラスタが実行されている名前空間で構成されたワークロード ネットワークのアドレス範囲から割り当てられた、それぞれ別の IP アドレスが割り当てられます。

IP アドレス範囲の割り当て

HA プロキシ ロード バランサを使用する スーパーバイザー のネットワーク トポロジを計画するときは、次の 2 種類の IP アドレス範囲を設定するように計画します。

- HAProxy に対する仮想 IP アドレスの割り当ての範囲。HAProxy の仮想サーバ用に構成した IP アドレス範囲は、ロード バランサ アプライアンスによって予約されます。たとえば、仮想 IP アドレス範囲が `192.168.1.0/24` の場合、この範囲に含まれるすべてのホストは、仮想 IP トラフィック以外のトラフィックではアクセスできません。

  注： HAProxy 仮想 IP アドレス範囲内にゲートウェイを構成するとゲートウェイへのすべてのルートが失敗するため、構成しないようにします。

- スーパーバイザー および Tanzu Kubernetes Grid クラスタのノードの IP アドレス範囲。スーパーバイザー内の Kubernetes 制御プレーン仮想マシンにはそれぞれ IP アドレスが割り当てられていて、合計で 3 つの IP アドレスがあります。Tanzu Kubernetes Grid クラスタの各ノードには、別の IP アドレスが割り当てられます。名前空間に構成する スーパーバイザー の各ワークロード ネットワークに、一意の IP アドレス範囲を割り当てる必要があります。

1 つの /24 ネットワークによる構成の例：

- ネットワーク：192.168.120.0/24
- HAProxy 仮想 IP アドレス：192.168.120.128/25
- HAProxy ワークロード インターフェイスの 1 つの IP アドレス：192.168.120.5

最初の 128 アドレスに含まれる制限のない IP アドレスに応じて、スーパーバイザー のワークロード ネットワークの IP アドレス範囲を定義できます。たとえば、次のようにします。

- 192.168.120.31 ～ 192.168.120.40：プライマリ ワークロード ネットワーク
- 192.168.120.51 ～ 192.168.120.60：別のワークロード ネットワーク

注： ワークロード ネットワークに定義する範囲は、HAProxy 仮想 IP アドレスの範囲と重複しないようにする必要があります。

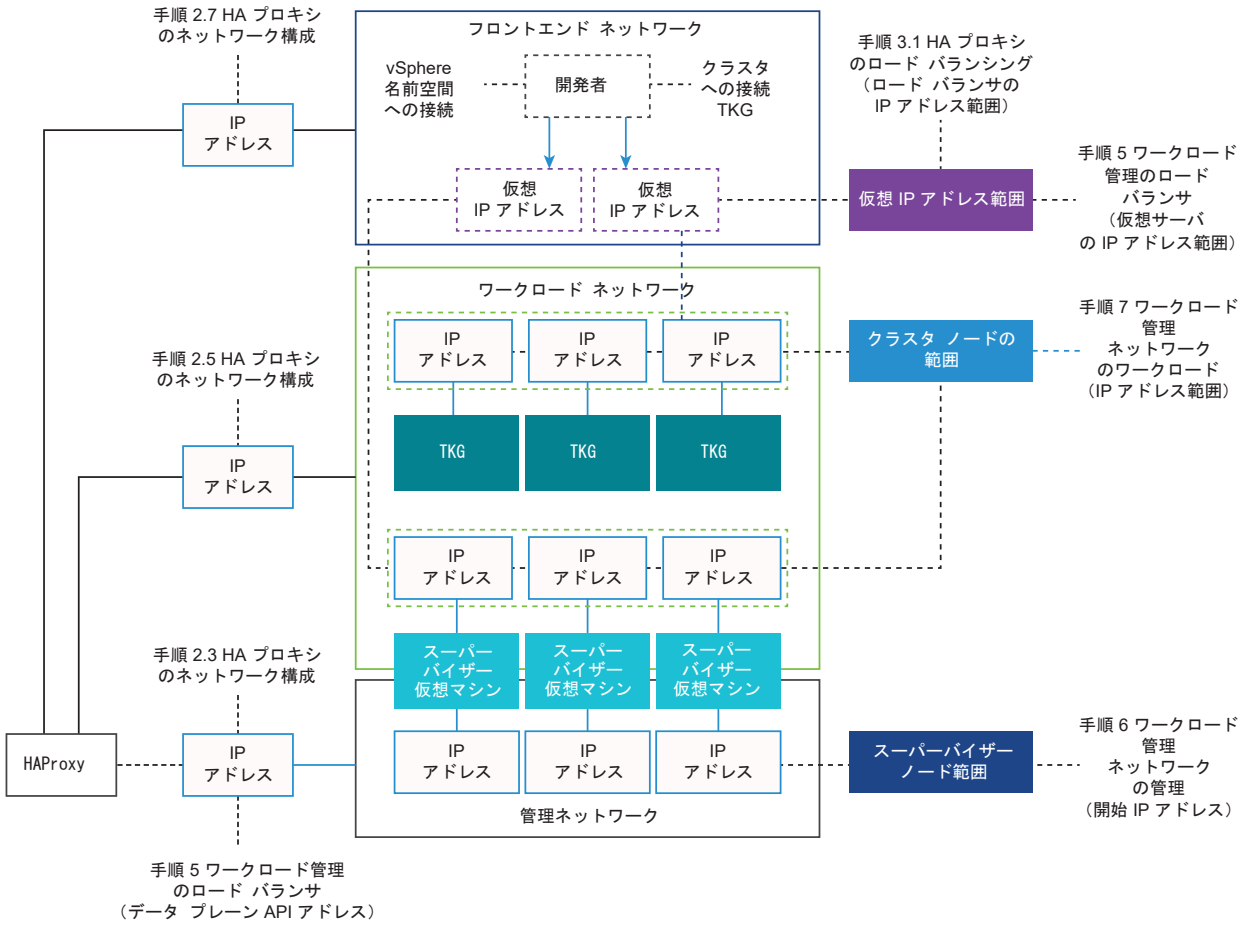
HAProxy ネットワーク トポロジ

ネットワーク構成には、[デフォルト] と [フロントエンド] という、HAProxy をデプロイする 2 つのオプションがあります。デフォルト ネットワークには、管理ネットワーク用とワークロード ネットワーク用の 2 つの NIC があります。フロントエンド ネットワークには、管理ネットワーク、ワークロード ネットワーク、クライアント用のフロントエンド ネットワークの 3 つの NIC があります。次の表に、各ネットワークの特性の一覧と説明を示します。

本番環境インストールでは、[フロントエンド ネットワーク] 構成を使用して HAProxy ロード バランサをデプロイすることが推奨されます。[デフォルト] 構成を使用して HAProxy ロード バランサをデプロイする場合は、ワークロード ネットワークに /24 の IP アドレス ブロック サイズを割り当てることをお勧めします。いずれの構成オプションでも、DHCP は推奨されません。

ネットワーク	特性
[管理]	スーパーバイザー クラスタは管理ネットワークを使用して HAProxy ロード バランサに接続し、このバランサをプログラムします。 ■ HAProxy データ プレーン API エンドポイントは、管理ネットワークに接続されているネットワーク インターフェイスにバインドされています。 ■ スーパーバイザー クラスタがロード バランサ API に確実に接続できるようにするには、HAProxy 制御プレーン仮想マシンに割り当てられた管理 IP アドレスに、管理ネットワーク上の固定 IP アドレスを指定する必要があります。 ■ HAProxy 仮想マシンのデフォルト ゲートウェイは、このネットワーク上に存在する必要があります。 ■ DNS クエリはこのネットワーク上で実行する必要があります。
[ワークロード]	HAProxy 制御プレーン仮想マシンは、ワークロード ネットワークを使用して、スーパーバイザー クラスタおよび Tanzu Kubernetes クラスタ ノードのサービスにアクセスします。 ■ HAProxy 制御プレーン仮想マシンは、このネットワーク上のスーパーバイザーおよび Tanzu Kubernetes クラスタ ノードにトラフィックを転送します。 ■ HAProxy 制御プレーン仮想マシンがデフォルト モード（2 つの NIC）でデプロイされている場合、ロード バランサ サービスへのアクセスに使用される論理ネットワークはワークロード ネットワークが提供する必要があります。 ■ [デフォルト] 構成では、ロードバランサの仮想 IP アドレスと Kubernetes クラスタ ノードの IP アドレスはこのネットワークから取得されます。これらのアドレスは、ネットワーク内の、重複しない、独立した範囲として定義されます。 **注：** ワークロード ネットワークは、管理ネットワークとは別のサブネットに配置してください。Distributed Switch ネットワークと HAProxy ロード バランサを使用したクラスタ スーパーバイザー のデプロイの要件を参照してください。
[フロントエンド]（オプション）	クラスタ ワークロードにアクセスする外部クライアント（ユーザーやアプリケーションなど）は、フロントエンド ネットワークを使用して、仮想 IP アドレスによってバックエンド ロード バランシング サービスにアクセスします。 ■ フロントエンド ネットワークが使用されるのは、HAProxy 制御プレーン仮想マシンが 3 つの NIC を使用してデプロイされている場合のみです。 ■ 本番環境インストールに推奨されます。 ■ フロントエンド ネットワークで、仮想 IP アドレス (VIP) が公開されます。HAProxy は、トラフィックのバランスを調整し、トラフィックを適切なバックエンドに転送します。

次の図に、[フロントエンド ネットワーク] トポロジを使用した HAProxy デプロイを示します。この図は、インストールおよび構成プロセスで想定される構成フィールドの場所を示しています。



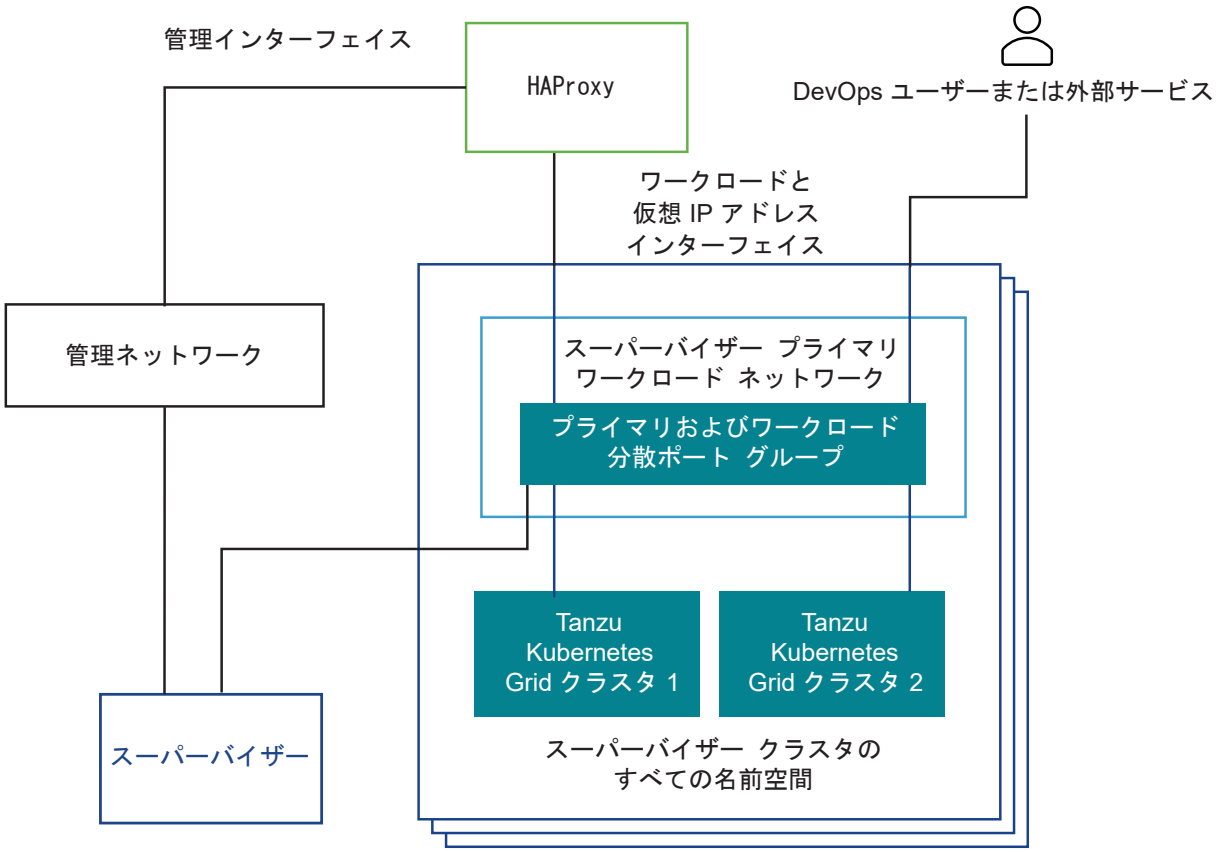
1 つのワークロード ネットワークを使用する スーパーバイザー トポロジと 2 つの仮想 NIC を使用する HAProxy

このトポロジでは、次のコンポーネントに対する 1 つのワークロード ネットワークを持つ スーパーバイザー を構成します。

- Kubernetes 制御プレーンの仮想マシン
- Tanzu Kubernetes Grid クラスタのノード。
- 外部サービスと DevOps ユーザーが接続する HAProxy の仮想 IP アドレス範囲。この構成では、2 つの仮想 NIC を使用する HAProxy がデプロイされます（[デフォルト] 構成）。1 つは管理ネットワークに接続され、もう 1 つはプライマリ ワークロード ネットワークに接続されます。仮想 IP アドレスは、プライマリ ワークロード ネットワークとは別のサブネットに割り当てる必要があります。

スーパーバイザー に対して 1 つのポート グループをプライマリ ワークロード ネットワークとして指定してから、同じポート グループを vSphere 名前空間 のワークロード ネットワークとして使用します。スーパーバイザー、Tanzu Kubernetes Grid クラスタ、HAProxy、DevOps ユーザー、および外部サービスはすべて、プライマリ ワークロード ネットワークとして設定されている同じ分散ポート グループに接続されます。

図 4-6. 1 つのネットワークによってバッキングされる スーパーバイザー



DevOps ユーザーまたは外部アプリケーションのトラフィック パスは次のとおりです。

1 DevOps ユーザーまたは外部サービスは、分散ポート グループのワークロード ネットワーク サブネット上の仮想 IP アドレスにトラフィックを送信します。

2 HAProxy は、仮想 IP トラフィックを Tanzu Kubernetes Grid クラスタ ノードの IP アドレス、または制御プレーン仮想マシンの IP アドレスのいずれかにロード バランシングします。HAProxy は、仮想 IP アドレスを要求して、その IP アドレスで受信されるトラフィックのロード バランシングを行うことができるようにします。

3 制御プレーン仮想マシンまたは Tanzu Kubernetes Grid クラスタ ノードは、スーパーバイザー または Tanzu Kubernetes Grid クラスタ内でそれぞれ実行されているターゲット ポッドにトラフィックを配信します。

隔離されたワークロード ネットワークを使用する スーパーバイザー トポロジと 2 つの仮想 NIC を使用する HA プロキシ

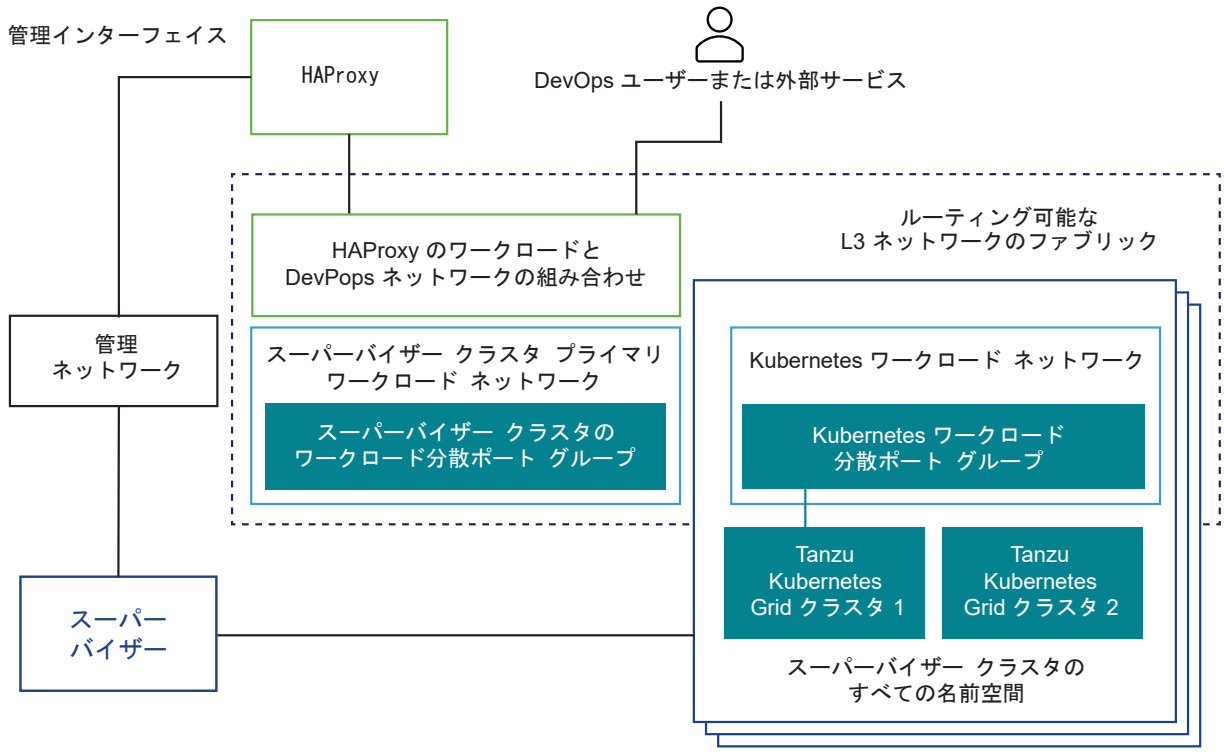
このトポロジでは、次のコンポーネントに対するネットワークを構成します。

- Kubernetes 制御プレーン仮想マシン。Kubernetes 制御プレーン仮想マシンのトラフィックを処理するプライマリ ワークロード ネットワーク。

- Tanzu Kubernetes Grid クラスタ ノード。ワークロード ネットワーク。これは、スーパーバイザー 上のすべての名前空間に割り当てられます。このネットワークは Tanzu Kubernetes Grid クラスタ ノードに接続します。
- HAProxy の仮想 IP アドレス。この構成では、2 つの仮想 NIC を使用する HAProxy 仮想マシンがデプロイされます（[デフォルト] 構成）。HAProxy 仮想マシンは、プライマリ ワークロード ネットワークか、名前空間に使用するワークロード ネットワークのいずれかに接続できます。また、HAProxy は、vSphere に既存の、プライマリ ネットワークおよびワークロード ネットワークにルーティング可能な仮想マシン ネットワークに接続することもできます。

スーパーバイザー は、プライマリ ワークロード ネットワークをバッキングする分散ポート グループに接続され、Tanzu Kubernetes Grid クラスタは、ワークロード ネットワークをバッキングする分散ポート グループに接続されます。2 つのポート グループは、レイヤー 3 でルーティング可能である必要があります。VLAN を使用してレイヤー 2 の隔離を実装できます。レイヤー 3 トラフィックのフィルタリングは、IP ファイアウォールとゲートウェイを介して実現できます。

図 4-7. 隔離されたワークロード ネットワークを使用する スーパーバイザー



DevOps ユーザーまたは外部サービスのトラフィック パスは次のとおりです。

1 DevOps ユーザーまたは外部サービスは、仮想 IP アドレスにトラフィックを送信します。トラフィックは、HAProxy が接続されているネットワークにルーティングされます。

2 HAProxy は、仮想 IP トラフィックを Tanzu Kubernetes Grid ノードの IP アドレス、または制御プレーン仮想マシンのいずれかにロード バランシングします。HAProxy は、仮想 IP アドレスを要求して、その IP アドレスで受信されるトラフィックのロードバランシングを行うことができるようにします。

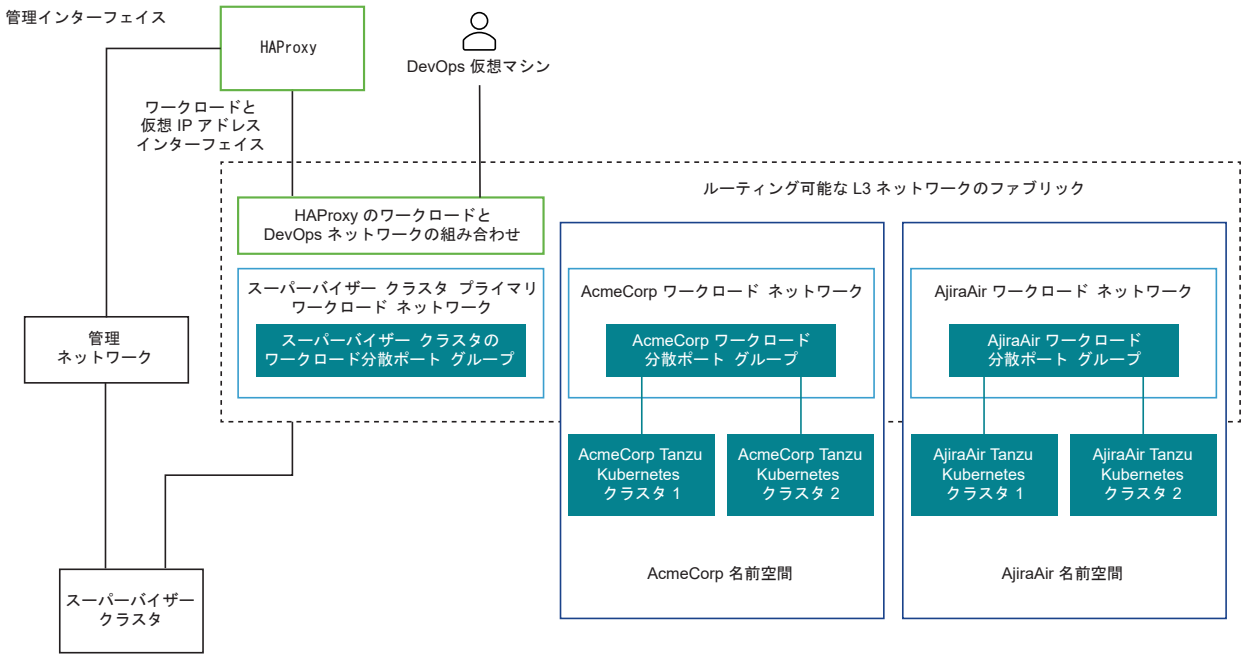
3 制御プレーン仮想マシンまたは Tanzu Kubernetes Grid クラスタ ノードは、Tanzu Kubernetes Grid クラスタ内で実行されているターゲット ポッドにトラフィックを配信します。

複数のワークロード ネットワークを使用する スーパーバイザー トポロジと 2 つの仮想 NIC を使用する HA プロキシ

このトポロジでは、1 つのポート グループがプライマリ ワークロード ネットワークとして動作するように、また、1 つの専用ポート グループが各名前空間に対するワークロード ネットワークとして機能するように構成できます。HAProxy は 2 つの仮想 NIC とともにデプロイされ（[デフォルト] 構成）、プライマリ ワークロード ネットワークか、いずれかのワークロード ネットワークに接続することができます。プライマリおよびワークロード ネットワークにルーティング可能な、既存の仮想マシン ネットワークを使用することもできます。

このトポロジの DevOps ユーザーと外部サービスのトラフィック パスは、隔離されたワークロード ネットワーク トポロジの場合と同じです。

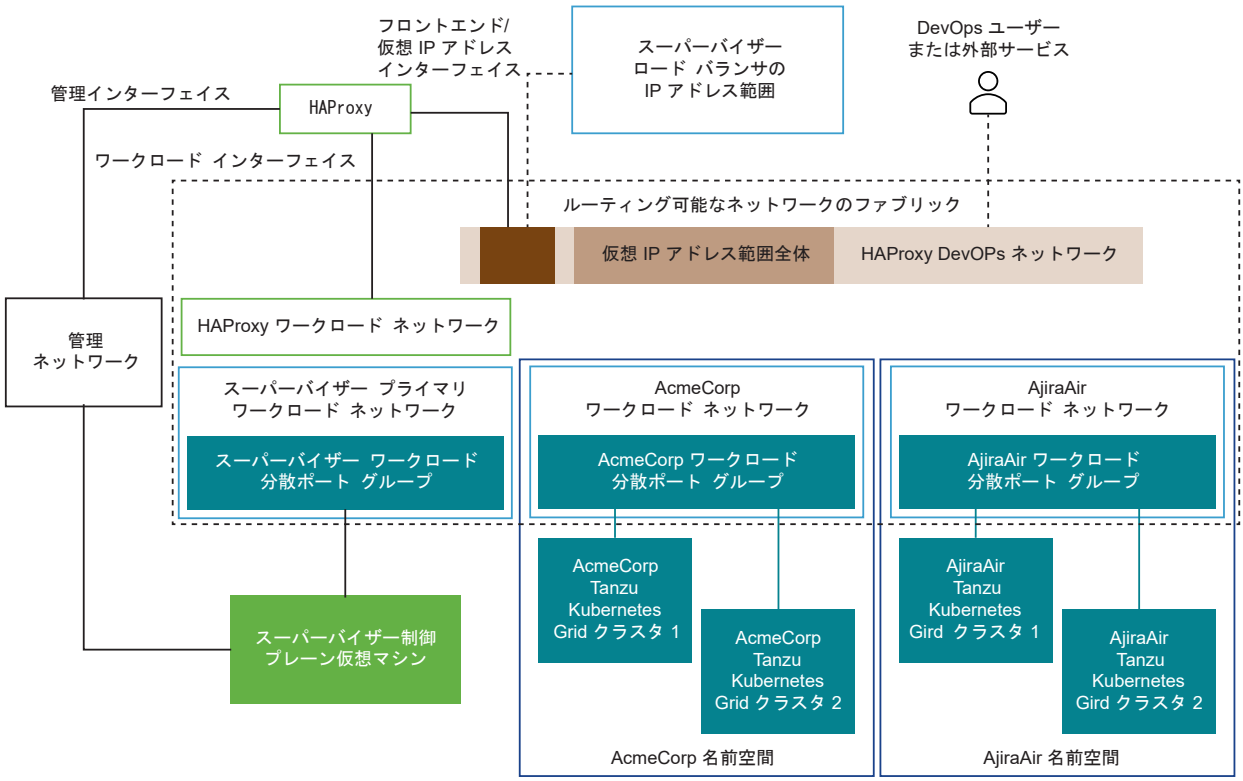
図 4-8. 複数の隔離されたワークロード ネットワークによってバッキングされる スーパーバイザー



複数のワークロード ネットワークを使用する スーパーバイザー トポロジと 3 つの仮想 NIC を使用する HA プロキシ

この構成では、3 つの仮想 NIC を使用する HAProxy 仮想マシンをデプロイします。これにより、HAProxy がフロントエンド ネットワークに接続されます。DevOps ユーザーと外部サービスは、フロントエンド ネットワーク上の仮想 IP アドレスを介して HAProxy にアクセスできます。本番環境では、3 つの仮想 NIC を使用する HA プロキシをデプロイすることを推奨します。

図 4-9. 3 つの仮想 NIC を使用する HAProxy をデプロイ



使用できるトポロジからの選択

使用できるトポロジから選択する前に、次のように環境のニーズを検討します。

1 スーパーバイザー と Tanzu Kubernetes Grid クラスタの間でレイヤー 2 の隔離が必要ですか。

   a いいえ：すべてのコンポーネントで使用される 1 つのワークロード ネットワークを持つ最もシンプルなトポロジ。

   b はい：分離されたプライマリ ネットワークとワークロード ネットワークを持つ、隔離ワークロード ネットワーク トポロジ。

2 Tanzu Kubernetes Grid クラスタの間でさらにレイヤー 2 の隔離が必要ですか。

   a いいえ：分離されたプライマリ ネットワークとワークロード ネットワークを持つ、隔離ワークロード ネットワーク トポロジ。

   b はい：名前空間ごとに分離されたワークロード ネットワークと専用のプライマリ ワークロード ネットワークを持つ、複数のワークロード ネットワーク トポロジ。

3 DevOps ユーザーと外部サービスが Kubernetes 制御プレーン仮想マシンと Tanzu Kubernetes Grid クラスタ ノードに直接ルーティングされないようにする必要がありますか?

   a いいえ：2 つの NIC を使用する HAProxy 構成。

   b はい：3 つの NIC を使用する HAProxy 構成。この構成は、本番環境に推奨されます。

vSphere IaaS control plane での HAProxy ロード バランサの使用に関する考慮事項

HAProxy ロード バランサを使用する vSphere IaaS control plane の運用を計画する場合は、次の考慮事項に注意します。

- HAProxy ロード バランサのテクニカル サポートを受けるには、HAProxy のサポート契約が必要です。VMware サポートでは HAProxy アプライアンスのサポートを提供できません。
- HAProxy アプライアンスは、高可用性トポロジに利用できないシングルトンです。高可用性環境の場合、VMware は、NSX または NSX Advanced Load Balancer のフル インストールのいずれかを使用することを推奨しています。
- フロントエンドに使用される IP アドレス範囲を後で拡張することはできません。ネットワークは将来の拡張に対応してサイジングする必要があります。

ゾーン スーパーバイザー デプロイの要件

5

vSphere Zone で スーパーバイザー を有効にするための要件を確認します。スーパーバイザー が有効な vSphere Zone では、vSphere クラスタ レベルの Kubernetes ワークロードに高可用性が提供されます。

注： vSphere IaaS control plane 環境を 8.0 よりも前のバージョンの vSphere からアップグレードした場合、Tanzu Kubernetes Grid クラスタなどの環境に vSphere Zone を使用するには、新しい 3 ゾーン スーパーバイザー を作成する必要があります。vSphere IaaS control plane では、単一クラスタから 3 ゾーンへの スーパーバイザー の変換はサポートされていません。

次のトピックを参照してください。

- NSX Advanced Load Balancer および Distributed Switch ネットワークを使用したゾーン スーパーバイザー デプロイの要件
- NSX でのゾーン スーパーバイザー の要件
- NSX および NSX Advanced Load Balancer でのゾーン スーパーバイザー の要件
- HA プロキシ ロード バランサを使用したゾーン スーパーバイザー デプロイの要件

NSX Advanced Load Balancer および Distributed Switch ネットワークを使用したゾーン スーパーバイザー デプロイの要件

3 つの vSphere Zone にマッピングされた 3 つの vSphere クラスタで Distributed Switch ネットワークと スーパーバイザー を使用して NSX Advanced Load Balancer を有効にするための要件を確認します。Avi Load Balancer とも呼ばれる NSX Advanced Load Balancer を使用して vSphere IaaS control plane を構成するには、使用環境が特定の要件を満たしている必要があります。vSphere IaaS control plane では複数のトポロジ（Avi サービス エンジンおよびロード バランサ サービス用の単一の Distributed Switch ネットワーク、Avi 管理プレーン用の Distributed Switch および NSX Advanced Load Balancer 用の別の Distributed Switch）がサポートされます。

ワークロード ネットワーク

Distributed Switch ネットワーク スタックを使用した スーパーバイザー を構成するには、クラスタ内のすべてのホストを Distributed Switch に接続する必要があります。スーパーバイザー 用に実装するトポロジに応じて、1 つ以上の分散ポート グループを作成します。作成したポート グループを、ワークロード ネットワークとして、vSphere 名前空間 に指定します。

ワークロード ネットワークは、Tanzu Kubernetes Grid クラスタのノード、仮想マシン サービス を使用して作成された仮想マシン、スーパーバイザー 制御プレーン仮想マシンへの接続を提供します。Kubernetes 制御プレーン仮想マシンに接続を提供するワークロード ネットワークは、プライマリ ワークロード ネットワークと呼ばれます。各 スーパーバイザー にそれぞれ 1 つのプライマリ ワークロード ネットワークが必要です。スーパーバイザー に対して、分散ポート グループの 1 つをプライマリ ワークロード ネットワークとして指定する必要があります。

スーパーバイザー 上の Kubernetes 制御プレーン仮想マシンは、プライマリ ワークロード ネットワークに割り当てられた IP アドレス範囲から 3 つの IP アドレスを使用します。Tanzu Kubernetes Grid クラスタの各ノードには、この Tanzu Kubernetes Grid クラスタが実行されている名前空間で構成されたワークロード ネットワークのアドレス範囲から割り当てられた、それぞれ別の IP アドレスが割り当てられます。

ネットワーク要件

NSX Advanced Load Balancer には、次の 2 つのルーティング可能なサブネットが必要です。

- 管理ネットワーク。管理ネットワークには、Avi Controller（別名、コントローラ）が配置されています。管理ネットワークは、コントローラに vCenter Server、ESXi ホスト、および スーパーバイザー 制御プレーン ノードへの接続を提供します。このネットワークには、Avi サービス エンジンの管理インターフェイスが配置されます。このネットワークには、Distributed Switch と分散ポート グループが必要です。
- データ ネットワーク。Avi サービス エンジン（別名、サービス エンジン）のデータ インターフェイスはこのネットワークに接続されます。ロード バランサの仮想 IP アドレス (VIP) は、このネットワークから割り当てられます。このネットワークには、Distributed Switch と分散ポート グループが必要です。ロード バランサをインストールする前に、Distributed Switch とポート グループを構成する必要があります。

IP アドレスの割り当て

コントローラとサービス エンジンは管理ネットワークに接続されます。NSX Advanced Load Balancer をインストールして構成する際に、各コントローラ仮想マシンのルーティング可能な固定 IP アドレスを指定します。

サービス エンジンでは DHCP を使用できます。DHCP を使用できない場合は、サービス エンジンの IP アドレス プールを構成できます。

複数の物理サイトにまたがる vSphere ゾーンの配置

サイト間の遅延が 100 ミリ秒を超えない限り、vSphere ゾーンを複数の物理サイトに分散できます。たとえば、vSphere ゾーンを 2 つのサイトに配置する場合、一方のサイトに vSphere ゾーンを 1 つ、もう一方のサイトに 2 つ配置して分散させることができます。

テストを目的とした場合のコンピューティングの最小要件

vSphere IaaS control plane の機能をテストする場合は、プラットフォームを最小限のテストベッドにデプロイできます。ただし、このようなテストベッドは本番スケールのワークロードの実行には適しておらず、クラスタ レベルの高可用性は得られないことに注意する必要があります。

表 5-1. テストを目的とした場合のコンピューティングの最小要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8.0	小	2	21 GB	290 GB
vSphere クラスタ	■ 3 つの vSphere クラスタ ■ 各 vSphere クラスタで vSphere DRS と HA が有効になっている。vSphere DRS は、完全自動化モードまたは一部自動化モードになっている必要があります。 ■ vSphere クラスタごとに構成された独立型のストレージとネットワーク。	該当なし	該当なし	該当なし
ESXi ホスト 8.0	vSphere クラスタごと： ■ vSAN を使用しない場合：1 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ、クラスタあたり 2 台の ESXi ホスト。 **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	ホストあたり 8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB
NSX Advanced Load Balancer コントローラ	Enterprise	4（小） 8（中） 24（大）	12 GB 24 GB 128 GB	128 GB 128 GB 128 GB

本番環境のコンピューティングの最小要件

次の表に、3 つの vSphere Zone で Distributed Switch ネットワークと NSX Advanced Load Balancer を使用して スーパーバイザー を有効にするためのコンピューティングの最小要件を示します。ベスト プラクティスとして、管理ドメインとワークロード ドメインを分離することを検討してください。ワークロード ドメインは、ワークロードが実行される スーパーバイザー をホストします。管理ドメインは、vCenter Server などのすべての管理コンポーネントをホストします。

表 5-2. コンピューティングの最小要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8.0	小	2	21 GB	290 GB
vSphere クラスタ	■ 3 つの vSphere クラスタ ■ 各 vSphere クラスタで vSphere DRS と HA が有効になっている。vSphere DRS は、完全自動化モードまたは一部自動化モードになっている必要があります。 ■ vSphere クラスタごとに構成された独立型のストレージとネットワーク。	該当なし	該当なし	該当なし
ESXi ホスト 8.0	vSphere クラスタごと： ■ vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ 4 台の ESXi ホスト（クラスタごと）。 **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	ホストあたり 8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB
NSX Advanced Load Balancer コントローラ	Enterprise 本番環境では、3 台の Controller 仮想マシンで構成されたクラスタをインストールすることを推奨します。HA 構成にするには、2 台以上のサービスエンジン仮想マシンが必要です。	4（小） 8（中） 24（大）	12 GB 24 GB 128 GB	128 GB 128 GB 128 GB

ネットワークの最小要件

次の表に、Distributed Switch ネットワークと NSX Advanced Load Balancer を使用して スーパーバイザーを有効にするための最小ネットワーク要件を示します。

表 5-3. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
レイヤー 2 デバイス	1	スーパーバイザー のトラフィックを処理する管理ネットワークは、スーパーバイザー のすべてのクラスタ部分について同じレイヤー 2 デバイス上にある必要があります。また、プライマリ ワークロード ネットワークも同じレイヤー 2 デバイス上にある必要があります。
物理ネットワークの MTU	1500	分散ポート グループの MTU サイズは 1500 以上にする必要があります。

表 5-4. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
遅延	100 ミリ秒	スーパーバイザー に結合されている vSphere Zone に含まれる各クラスタ間の最大推奨最大遅延。
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP)

表 5-5. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。
管理ネットワークのサブネット	1	管理ネットワークには、NSX Advanced Load Balancer Controller（別名、コントローラ）が配置されています。 また、サービス エンジン管理インターフェイスも接続されます。Controller は、このネットワーク内の vCenter Server および ESXi 管理 IP アドレスに接続する必要があります **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。

表 5-6. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere Distributed Switch	1	3 つすべての vSphere クラスタのすべてのホストを Distributed Switch に接続する必要があります。
ワークロード ネットワーク	1	プライマリ ワークロード ネットワークとして構成する Distributed Switch には、1 つ以上の分散ポート グループを作成する必要があります。選択したトポロジによっては、名前空間のワークロード ネットワークと同じ分散ポート グループを使用することや、追加のポート グループを作成してワークロード ネットワークとして構成することができます。ワークロード ネットワークは次の要件を満たす必要があります。 ■ 任意のワークロード ネットワークと、NSX Advanced Load Balancer が仮想 IP アドレスの割り当てに使用するネットワークとの間でルーティングできること。 ■ スーパーバイザー 内のすべてのワークロード ネットワークで IP アドレス範囲の重複がないこと。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

表 5-7. ロード バランサ ネットワークの要件

NTP サーバおよび DNS サーバ	1	NSX Advanced Load Balancer Controller で vCenter Server と ESXi のホスト名が正しく解決されるようにするには、DNS サーバの IP アドレスが必要です。パブリック NTP サーバはデフォルトで使用されるため、NTP は省略可能です。
データ ネットワークのサブネット	1	サービス エンジン（別名、サービス エンジン）のデータ インターフェイスはこのネットワークに接続されます。サービス エンジンの IP アドレス プールを構成します。ロード バランサの仮想 IP アドレス (VIP) は、このネットワークから割り当てられます。

表 5-7. ロード バランサ ネットワークの要件 （続き）

NSX Advanced Load Balancer Controller の IP アドレス	1 または 4	NSX Advanced Load Balancer Controller を単一ノードとしてデプロイする場合、その管理インターフェイス用に 1 つの固定 IP アドレスが必要です。 3 ノード クラスタの場合は、4 つの IP アドレスが必要です。各 Controller 仮想マシンに 1 つ、クラスタ仮想 IP アドレスに 1 つです。これらの IP アドレスは、管理ネットワーク サブネットから取得する必要があります。
VIP IP アドレス管理の範囲	-	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。IP アドレスは、データ ネットワーク サブネットから取得する必要があります。スーパーバイザー クラスタごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

ポートとプロトコル

次の表に、NSX Advanced Load Balancer、 vCenter Server とその他の vSphere IaaS control plane コンポーネント間の IP 接続を管理するために必要なプロトコルとポートを示します。

ソース	ターゲット	プロトコルとポート
NSX Advanced Load Balancer コントローラ	NSX Advanced Load Balancer Controller（クラスタ内）	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
サービス エンジン	HA のサービス エンジン	TCP 9001（VMware、LSC、NSX-T クラウド用）
サービス エンジン	NSX Advanced Load Balancer コントローラ	TCP 22 (SSH) TCP 8443 (HTTPS) UDP 123 (NTP)
NSX Advanced Load Balancer コントローラ	vCenter Server、ESXi、NSX-T Manager	TCP 443 (HTTPS)
スーパーバイザー制御プレーンノード (AKO)	NSX Advanced Load Balancer コントローラ	TCP 443 (HTTPS)

NSX Advanced Load Balancer のポートとプロトコルの詳細については、https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer を参照してください。

NSX でのゾーン スーパーバイザー の要件

NSX ネットワーク スタックを使用して、vSphere Zone にマッピングされた 3 つの vSphere クラスタで スーパーバイザー を有効にするためのシステム要件を確認します。

これらの要件に加えて、NSX のデプロイに関するベスト プラクティスの詳細については、『NSX Reference Design Guide』を参照してください。

複数の物理サイトにまたがる vSphere ゾーンの配置

サイト間の遅延が 100 ミリ秒を超えない限り、vSphere ゾーンを複数の物理サイトに分散できます。たとえば、vSphere ゾーンを 2 つのサイトに配置する場合、一方のサイトに vSphere ゾーンを 1 つ、もう一方のサイトに 2 つ配置して分散させることができます。

管理クラスタと Edge クラスタの最小コンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8	小	2	21 GB	290 GB
ESXi ホスト 8	2 台の ESXi ホスト	8	ホストあたり 64 GB	該当なし
NSX Manager	中	6	24 GB	300 GB
NSX Edge 1	大	8	32 GB	200 GB
NSX Edge 2	大	8	32 GB	200 GB

注： vSphere IaaS control plane を構成する vSphere クラスタに参加しているすべての ESXi ホストが、NSX トランスポート ノードとして準備されていることを確認します。詳細については、NSX ドキュメントの「トランスポート ノードとしての ESXi ホストの準備」と https://kb.vmware.com/s/article/95820 を参照してください。

ワークロード ドメイン クラスタの最小コンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vSphere クラスタ	■ 3 つの vSphere クラスタ ■ 各 vSphere クラスタで vSphere DRS と HA が有効になっている。vSphere DRS は、完全自動化モードになっている必要があります。 ■ vSphere クラスタごとに構成された独立型のストレージとネットワーク。	該当なし	該当なし	該当なし
ESXi ホスト 8	vSphere クラスタごと： ■ vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ 4 台の ESXi ホスト（クラスタごと）。 **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB

ネットワーク要件

注： vSphere 8 スーパーバイザー による IPv6 クラスタの作成や、Tanzu Mission Control による IPv6 クラスタの登録はできません。

VMware 製品の相互運用性マトリックスで、サポート対象の NSX のバージョンを確認します。

表 5-8. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
レイヤー 2 デバイス	1	スーパーバイザー のトラフィックを処理する管理ネットワークは、同じレイヤー 2 デバイス上にある必要があります。管理トラフィックを処理するホストごとに、1 つ以上の物理 NIC を同じレイヤー 2 デバイスに接続する必要があります。
物理ネットワークの MTU	1500	vSphere Distributed Switch ポート グループの MTU サイズは 1500 以上にする必要があります。
物理 NIC	vSAN が使用されている場合は、ホストあたり 2 つ以上の物理 NIC	Antrea CNI を使用し、最適な NSX パフォーマンスを得るには、参加している各 ESXi ホスト上の各物理 NIC で GENEVE カプセル化がサポートされていること、および GENEVE カプセル化を有効にすることが必要です。

表 5-9. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
遅延	100 ミリ秒	スーパーバイザー に結合されている vSphere Zone に含まれる各クラスタ間の最大推奨最大遅延。
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP)
イメージ レジストリ	1	サービスのレジストリへのアクセス。

表 5-10. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。
管理ネットワークのサブネット	1	ESXi ホストと、vCenter Server、NSX アプライアンス、および Kubernetes 制御プレーンとの間の管理トラフィックに使用されるサブネット。サブネットのサイズは次のようにする必要があります。 ■ ホストの VMkernel アダプタごとに 1 つの IP アドレス。 ■ vCenter Server アプライアンスに 1 つの IP アドレス。 ■ NSX Manager に 1 つまたは 4 つの IP アドレス。3 台のノードと 1 つの仮想 IP アドレス (VIP) の NSX Manager クラスタリングを実行する場合は 4 つです。 ■ Kubernetes 制御プレーンに 5 つの IP アドレス。3 台のノードそれぞれに 1 つずつ、仮想 IP アドレス用に 1 つ、クラスタのローリング アップグレード用に 1 つ。 **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。
管理ネットワークの VLAN	1	管理ネットワークのサブネットの VLAN ID。

表 5-11. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere ポッド CIDR 範囲	/23 プライベート IP アドレス	vSphere ポッド の IP アドレスを提供するプライベート CIDR 範囲。これらのアドレスは、Tanzu Kubernetes Grid クラスタ ノードにも使用されます。 クラスタごとに一意の vSphere ポッド CIDR 範囲を指定する必要があります。 **注：** vSphere ポッド の CIDR 範囲と、Kubernetes サービス アドレスの CIDR 範囲が重複しないようにする必要があります。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。
出力方向 CIDR の範囲	/27 固定 IP アドレス	Kubernetes サービスの出力方向 IP アドレスを決定するプライベート CIDR 注釈。スーパーバイザー 内の名前空間ごとに 1 つの出力方向 IP アドレスのみが割り当てられます。出力方向 IP アドレスは、外部エンティティが名前空間内のサービスとの通信に使用するアドレスです。出力方向 IP アドレスの数によって、スーパーバイザー で保持できる出力方向ポリシーの数が制限されます。 最小値は /27 以上の CIDR です。たとえば、`10.174.4.96/27`。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
入力方向 CIDR	/27 固定 IP アドレス	入力方向の IP アドレスに使用されるプライベート CIDR 範囲。入力方向を使用すると、外部ネットワークから スーパーバイザー に送信される要求にトラフィック ポリシーを適用できます。入力方向 IP アドレスの数によって、クラスタで保持できる入力の数が制限されます。 最小値は /27 以上の CIDR です。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
名前空間ネットワーク範囲	1	サブネット/セグメントを作成し、ワークロードに IP アドレスを割り当てる 1 つ以上の IP CIDR。
名前空間サブネット プリフィックス	1	名前空間セグメント用に予約されるサブネットのサイズを指定するサブネット プリフィックス。デフォルトは 28 です。

表 5-12. NSX の要件

コンポーネント	最小数	V
VLAN	3	VLAN IP アドレスはトンネル エンドポイント (TEP) の IP アドレスです。ESXi ホスト TEP と Edge TEP はルーティング可能である必要があります。 VLAN IP アドレスが必要となるものは次のとおりです。 ■ ESXi ホスト VTEP ■ 固定 IP アドレスを使用する Edge VTEP ■ トランスポート ノードの Tier-0 ゲートウェイとアップリンク。 **注：** ESXi ホスト VTEP および Edge VTEP では、MTU サイズを 1,600 よりも大きくする必要があります。 ESXi ホストおよび NSX-T Edge ノードはトンネル エンドポイントとして機能し、各ホストおよび Edge ノードにトンネル エンドポイント (TEP) IP アドレスが割り当てられます。 ESXi ホストの TEP IP アドレスは Edge ノードの TEP IP アドレスとのオーバーレイ トンネルを確立するため、VLAN IP アドレスはルーティング可能である必要があります。 Tier-0 ゲートウェイへの North-South 接続を提供するには、追加の VLAN が必要です。 IP アドレス プールはクラスタ間で共有できます。ただし、ホスト オーバーレイの IP アドレス プール/VLAN を Edge オーバーレイの IP アドレス プール/VLAN と共有することはできません。 **注：** ホスト TEP と Edge TEP が異なる物理 NIC を使用している場合、同じ VLAN を使用できます。
Tier-0 アップリンクの IP アドレス	/24 プライベート IP アドレス	Tier 0 アップリンクに使用される IP サブネット。Tier 0 アップリンクの IP アドレスの要件は次のとおりです。 ■ 1 つの IP アドレス：Edge の冗長性を使用しない場合。 ■ 4 つの IP アドレス：BGP と Edge の冗長性を使用する場合。Edge ごとに 2 つの IP アドレス。 ■ 3 つの IP アドレス：スタティック ルートと Edge の冗長性を使用する場合。 Edge 管理の IP アドレス、サブネット、ゲートウェイ、アップリンクの IP アドレス、サブネット、ゲートウェイは一意である必要があります。

NSX および NSX Advanced Load Balancer でのゾーン スーパーバイザー の要件

NSX ネットワーク スタックと NSX Advanced Load Balancer を使用して、vSphere Zone にマッピングされた 3 つの vSphere クラスタで スーパーバイザー を有効にするためのシステム要件を確認します。

複数の物理サイトにまたがる vSphere ゾーンの配置

サイト間の遅延が 100 ミリ秒を超えない限り、vSphere ゾーンを複数の物理サイトに分散できます。たとえば、vSphere ゾーンを 2 つのサイトに配置する場合、一方のサイトに vSphere ゾーンを 1 つ、もう一方のサイトに 2 つ配置して分散させることができます。

NSX デプロイのオプション

NSX をデプロイする際のベスト プラクティスの詳細については、『NSX Reference Design Guide』を参照してください。

管理クラスタと Edge クラスタの最小コンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8	小	2	21 GB	290 GB
ESXi ホスト 8	2 台の ESXi ホスト	8	ホストあたり 64 GB	該当なし
NSX Manager	中	6	24 GB	300 GB
NSX Edge 1	大	8	32 GB	200 GB
NSX Edge 2	大	8	32 GB	200 GB
サービス エンジン仮想マシン	スーパーバイザー ごとに少なくとも 2 台のサービス エンジン仮想マシンがデプロイされます	1	2 GB	該当なし

注： vSphere IaaS control plane を構成する vSphere クラスタに参加しているすべての ESXi ホストが、NSX トランスポート ノードとして準備されていることを確認します。詳細については、NSX ドキュメントの「トランスポート ノードとしての ESXi ホストの準備」と https://kb.vmware.com/s/article/95820 を参照してください。

コントローラのシステム キャパシティの指定

デプロイ時にコントローラのシステム キャパシティを指定できます。システム キャパシティは、CPU、RAM、ディスクなどシステム リソースの割り当てに基づきます。割り当てるリソースの量はコントローラのパフォーマンスに影響します。

デプロイ タイプ	ノード数	推奨される割り当て - CPU	推奨される割り当て - メモリ	推奨される割り当て - ディスク
デモ/ユーザーによる評価	1	6	24 GB	128 GB

デモ用デプロイでは、単一のコントローラが適切です。すべての制御プレーン アクティビティとワークフロー、および分析に単一のコントローラが使用されます。

本番デプロイでは、3 ノードのクラスタが推奨されます。

詳細については、「NSX Advanced Load Balancer Controller のサイジング」を参照してください。

ワークロード ドメイン クラスタの最小コンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vSphere クラスタ	■ 3 つの vSphere クラスタ ■ 各 vSphere クラスタで vSphere DRS と HA が有効になっている。vSphere DRS は、完全自動化モードになっている必要があります。 ■ vSphere クラスタごとに構成された独立型のストレージとネットワーク。	該当なし	該当なし	該当なし
ESXi ホスト 8	vSphere クラスタごと： ■ vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ 4 台の ESXi ホスト（クラスタごと）。 **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB

ネットワーク要件

注： vSphere 8 スーパーバイザー による IPv6 クラスタの作成や、Tanzu Mission Control による IPv6 クラスタの登録はできません。

VMware 製品の相互運用性マトリックスで、サポート対象の NSX のバージョンを確認します。

表 5-13. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
レイヤー 2 デバイス	1	スーパーバイザー のトラフィックを処理する管理ネットワークは、同じレイヤー 2 デバイス上にある必要があります。管理トラフィックを処理するホストごとに、1 つ以上の物理 NIC を同じレイヤー 2 デバイスに接続する必要があります。
物理ネットワークの MTU	1,700	vSphere Distributed Switch ポート グループの MTU サイズは 1,700 以上にする必要があります。
物理 NIC	vSAN が使用されている場合は、ホストあたり 2 つ以上の物理 NIC	Antrea CNI を使用し、最適な NSX パフォーマンスを得るには、参加している各 ESXi ホスト上の各物理 NIC で GENEVE カプセル化がサポートされていること、および GENEVE カプセル化を有効にすることが必要です。

表 5-14. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
遅延	100 ミリ秒	スーパーバイザー に結合されている vSphere Zone に含まれる各クラスタ間の最大推奨最大遅延。
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP)
イメージ レジストリ	1	サービスのレジストリへのアクセス。

表 5-15. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。
管理ネットワークのサブネット	1	ESXi ホストと、vCenter Server、NSX アプライアンス、および Kubernetes 制御プレーンとの間の管理トラフィックに使用されるサブネット。サブネットのサイズは次のようにする必要があります。 ■ ホストの VMkernel アダプタごとに 1 つの IP アドレス。 ■ vCenter Server アプライアンスに 1 つの IP アドレス。 ■ NSX Manager に 1 つまたは 4 つの IP アドレス。3 台のノードと 1 つの仮想 IP アドレス (VIP) の NSX Manager クラスタリングを実行する場合は 4 つです。 ■ Kubernetes 制御プレーンに 5 つの IP アドレス。3 台のノードそれぞれに 1 つずつ、仮想 IP アドレス用に 1 つ、クラスタのローリング アップグレード用に 1 つ。 **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。
管理ネットワークの VLAN	1	管理ネットワークのサブネットの VLAN ID。

表 5-16. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere ポッド CIDR 範囲	/23 プライベート IP アドレス	vSphere ポッド の IP アドレスを提供するプライベート CIDR 範囲。これらのアドレスは、Tanzu Kubernetes Grid クラスタ ノードにも使用されます。 クラスタごとに一意の vSphere ポッド CIDR 範囲を指定する必要があります。 **注：** vSphere ポッド の CIDR 範囲と、Kubernetes サービス アドレスの CIDR 範囲が重複しないようにする必要があります。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。
出力方向 CIDR の範囲	/27 固定 IP アドレス	Kubernetes サービスの出力方向 IP アドレスを決定するプライベート CIDR 注釈。スーパーバイザー 内の名前空間ごとに 1 つの出力方向 IP アドレスのみが割り当てられます。出力方向 IP アドレスは、外部エンティティが名前空間内のサービスとの通信に使用するアドレスです。出力方向 IP アドレスの数によって、スーパーバイザー で保持できる出力方向ポリシーの数が制限されます。 最小値は /27 以上の CIDR です。たとえば、`10.174.4.96/27`。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
入力方向 CIDR	/27 固定 IP アドレス	入力方向の IP アドレスに使用されるプライベート CIDR 範囲。入力方向を使用すると、外部ネットワークから スーパーバイザー に送信される要求にトラフィック ポリシーを適用できます。入力方向 IP アドレスの数によって、クラスタで保持できる入力の数が制限されます。 最小値は /27 以上の CIDR です。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
名前空間ネットワーク範囲	1	サブネット/セグメントを作成し、ワークロードに IP アドレスを割り当てる 1 つ以上の IP CIDR。
名前空間サブネット プリフィックス	1	名前空間セグメント用に予約されるサブネットのサイズを指定するサブネット プリフィックス。デフォルトは 28 です。

表 5-17. NSX の要件

コンポーネント	最小数	V
VLAN	3	VLAN IP アドレスはトンネル エンドポイント (TEP) の IP アドレスです。ESXi ホスト TEP と Edge TEP はルーティング可能である必要があります。 VLAN IP アドレスが必要となるものは次のとおりです。 ■ ESXi ホスト VTEP ■ 固定 IP アドレスを使用する Edge VTEP ■ トランスポート ノードの Tier-0 ゲートウェイとアップリンク。 **注：** ESXi ホスト VTEP および Edge VTEP では、MTU サイズを 1,600 よりも大きくする必要があります。 ESXi ホストおよび NSX-T Edge ノードはトンネル エンドポイントとして機能し、各ホストおよび Edge ノードにトンネル エンドポイント (TEP) IP アドレスが割り当てられます。 ESXi ホストの TEP IP アドレスは Edge ノードの TEP IP アドレスとのオーバーレイ トンネルを確立するため、VLAN IP アドレスはルーティング可能である必要があります。 Tier-0 ゲートウェイへの North-South 接続を提供するには、追加の VLAN が必要です。 IP アドレス プールはクラスタ間で共有できます。ただし、ホスト オーバーレイの IP アドレス プール/VLAN を Edge オーバーレイの IP アドレス プール/VLAN と共有することはできません。 **注：** ホスト TEP と Edge TEP が異なる物理 NIC を使用している場合、同じ VLAN を使用できます。
Tier-0 アップリンクの IP アドレス	/24 プライベート IP アドレス	Tier 0 アップリンクに使用される IP サブネット。Tier 0 アップリンクの IP アドレスの要件は次のとおりです。 ■ 1 つの IP アドレス：Edge の冗長性を使用しない場合。 ■ 4 つの IP アドレス：BGP と Edge の冗長性を使用する場合。Edge ごとに 2 つの IP アドレス。 ■ 3 つの IP アドレス：スタティック ルートと Edge の冗長性を使用する場合。 Edge 管理の IP アドレス、サブネット、ゲートウェイ、アップリンクの IP アドレス、サブネット、ゲートウェイは一意である必要があります。

表 5-18. ロード バランサ ネットワークの要件

NTP サーバおよび DNS サーバ	1	NSX Advanced Load Balancer Controller で vCenter Server と ESXi のホスト名が正しく解決されるようにするには、DNS サーバの IP アドレスが必要です。パブリック NTP サーバはデフォルトで使用されるため、NTP は省略可能です。
データ ネットワークのサブネット	1	サービス エンジン（別名、サービス エンジン）のデータ インターフェイスはこのネットワークに接続されます。サービス エンジンの IP アドレス プールを構成します。ロード バランサの仮想 IP アドレス (VIP) は、このネットワークから割り当てられます。
NSX Advanced Load Balancer Controller の IP アドレス	1 または 4	NSX Advanced Load Balancer Controller を単一ノードとしてデプロイする場合、その管理インターフェイス用に 1 つの固定 IP アドレスが必要です。 3 ノード クラスタの場合は、4 つの IP アドレスが必要です。各 Controller 仮想マシンに 1 つ、クラスタ仮想 IP アドレスに 1 つです。これらの IP アドレスは、管理ネットワーク サブネットから取得する必要があります。
VIP IP アドレス管理の範囲	-	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。IP アドレスは、データ ネットワーク サブネットから取得する必要があります。スーパーバイザー クラスタごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

ポートとプロトコル

次の表に、NSX Advanced Load Balancer、 vCenter Server とその他の vSphere IaaS control plane コンポーネント間の IP 接続を管理するために必要なプロトコルとポートを示します。

ソース	ターゲット	プロトコルとポート
NSX Advanced Load Balancer コントローラ	NSX Advanced Load Balancer Controller（クラスタ内）	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
サービス エンジン	HA のサービス エンジン	TCP 9001（VMware、LSC、NSX-T クラウド用）
サービス エンジン	NSX Advanced Load Balancer コントローラ	TCP 22 (SSH) TCP 8443 (HTTPS) UDP 123 (NTP)

ソース	ターゲット	プロトコルとポート
NSX Advanced Load Balancer コントローラ	vCenter Server、ESXi、NSX-T Manager	TCP 443 (HTTPS)
スーパーバイザー制御プレーンノード (AKO)	NSX Advanced Load Balancer コントローラ	TCP 443 (HTTPS)

NSX Advanced Load Balancer のポートとプロトコルの詳細については、https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer を参照してください。

HA プロキシ ロード バランサを使用したゾーン スーパーバイザー デプロイの要件

vSphere ゾーンにマッピングされた 3 つの vSphere クラスタで Distributed Switch ネットワークと HAProxy ロード バランサを使用して スーパーバイザー を有効にするための要件を確認します。

複数の物理サイトにまたがる vSphere ゾーンの配置

サイト間の遅延が 100 ミリ秒を超えない限り、vSphere ゾーンを複数の物理サイトに分散できます。たとえば、vSphere ゾーンを 2 つのサイトに配置する場合、一方のサイトに vSphere ゾーンを 1 つ、もう一方のサイトに 2 つ配置して分散させることができます。

コンピューティングの最小要件

次の表に、3 つの vSphere Zone で Distributed Switch ネットワークと HA プロキシ ロード バランサを使用して スーパーバイザー を有効にするための最小コンピューティング要件を示します。ベスト プラクティスとして、管理ドメインとワークロード ドメインを分離することを検討してください。ワークロード ドメインは、ワークロードが実行される スーパーバイザー をホストします。管理ドメインは、vCenter Server などのすべての管理コンポーネントをホストします。

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8.0	小	2	21 GB	290 GB
vSphere クラスタ	■ 3 つの vSphere クラスタ ■ 各 vSphere クラスタで vSphere DRS と HA が有効になっている。vSphere DRS は、完全自動化モードまたは一部自動化モードになっている必要があります。 ■ vSphere クラスタごとに構成された独立型のストレージとネットワーク。	該当なし	該当なし	該当なし

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
ESXi ホスト 8.0	vSphere クラスタごと： ■ vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ、クラスタあたり 4 台の ESXi ホスト。 **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB

ネットワークの最小要件

注： vSphere 8 スーパーバイザー による IPv6 クラスタの作成や、Tanzu Mission Control による IPv6 クラスタの登録はできません。

表 5-19. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
レイヤー 2 デバイス	1	スーパーバイザー のトラフィックを処理する管理ネットワークは、スーパーバイザー のすべてのクラスタ部分について同じレイヤー 2 デバイス上にある必要があります。また、プライマリ ワークロード ネットワークも同じレイヤー 2 デバイス上にある必要があります。
物理ネットワークの MTU	1500	分散ポート グループの MTU サイズは 1500 以上にする必要があります。

表 5-20. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
遅延	100 ミリ秒	スーパーバイザー に結合されている vSphere Zone に含まれる各クラスタ間の最大推奨最大遅延。
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP)

表 5-21. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。

表 5-21. 管理ネットワークの要件 （続き）

コンポーネント	最小数	必要な構成
管理ネットワークのサブネット	1	ESXi ホストおよび vCenter Server と Kubernetes 制御プレーンとの間の管理トラフィックに使用されるサブネット。サブネットのサイズは次のようにする必要があります。 ■ ホストの VMkernel アダプタごとに 1 つの IP アドレス。 ■ vCenter Server アプライアンスに 1 つの IP アドレス。 ■ Kubernetes 制御プレーンに 5 つの IP アドレス。3 台のノードそれぞれに 1 つずつ、仮想 IP アドレス用に 1 つ、クラスタのローリング アップグレード用に 1 つ。 **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。
管理ネットワークの VLAN	1	管理ネットワークのサブネットの VLAN ID。

表 5-22. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere Distributed Switch	1	3 つすべての vSphere クラスタのすべてのホストを Distributed Switch に接続する必要があります。
ワークロード ネットワーク	1	プライマリ ワークロード ネットワークとして構成する Distributed Switch には、1 つ以上の分散ポート グループを作成する必要があります。選択したトポロジによっては、名前空間のワークロード ネットワークと同じ分散ポート グループを使用することや、追加のポート グループを作成してワークロード ネットワークとして構成することができます。ワークロード ネットワークは次の要件を満たす必要があります。 ■ 任意のワークロード ネットワークと、HAProxy が仮想 IP アドレスの割り当てに使用するネットワークとの間でルーティングできること。 ■ スーパーバイザー 内のすべてのワークロード ネットワークで IP アドレス範囲の重複がないこと。 **重要：** ワークロード ネットワークは、管理ネットワークとは別のサブネットに配置してください。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

表 5-23. ロード バランサ ネットワークの要件

HAProxy ロード バランサ	1	vCenter Server インスタンスで構成された HAProxy ロード バランサのインスタンス。 ■ 1 つの HAProxy インスタンスが複数の スーパーバイザー で使用されている場合、すべての スーパーバイザー のすべてのワークロード ネットワークとの間で、トラフィックをルーティングできる必要があります。 ■ HAProxy を使用するすべての スーパーバイザー のワークロード ネットワークにまたがる IP アドレス範囲は、重複しないようにする必要があります。 ■ HAProxy が仮想 IP アドレスを割り当てるために使用するネットワークは、この HAProxy が接続されているすべての スーパーバイザー で使用されるワークロード ネットワークにルーティング可能である必要があります。
仮想サーバの IP アドレス範囲	1	仮想 IP アドレスの専用 IP アドレス範囲。HAProxy 仮想マシンは、この仮想 IP アドレス範囲の唯一の所有者である必要があります。この範囲は、どの スーパーバイザー が所有するワークロード ネットワークに割り当てられた IP アドレス範囲とも重複が許されません。また、管理ネットワークと同じサブネット上にあってはなりません。

クラスタ スーパーバイザー デプロイの要件

6

1 つの vSphere Zone にマッピングされる単一の vSphere クラスタで スーパーバイザー を有効にするための要件を確認します。

次のトピックを参照してください。

- スーパーバイザー および Distributed Switch ネットワークを使用したクラスタ NSX Advanced Load Balancer デプロイの要件
- NSX を使用したクラスタ スーパーバイザー のデプロイの要件
- NSX および NSX Advanced Load Balancer を使用したクラスタ スーパーバイザー のデプロイの要件
- Distributed Switch ネットワークと HAProxy ロード バランサを使用したクラスタ スーパーバイザー のデプロイの要件

スーパーバイザー および Distributed Switch ネットワークを使用したクラスタ NSX Advanced Load Balancer デプロイの要件

Distributed Switch ネットワークと NSX Advanced Load Balancer（Avi Load Balancer とも呼ばれる）を使用して、vSphere クラスタで スーパーバイザー を有効にするための要件を確認します。vSphere IaaS control plane では複数のトポロジ（Avi サービス エンジンおよびロード バランサ サービス用の単一の Distributed Switch ネットワーク、Avi 管理プレーン用の Distributed Switch および NSX Advanced Load Balancer 用の別の Distributed Switch）がサポートされます。

ワークロード ネットワーク

Distributed Switch ネットワーク スタックを使用した スーパーバイザー を構成するには、クラスタ内のすべてのホストを Distributed Switch に接続する必要があります。スーパーバイザー 用に実装するトポロジに応じて、1 つ以上の分散ポート グループを作成します。作成したポート グループを、ワークロード ネットワークとして、vSphere 名前空間 に指定します。ワークロード ネットワークは、Tanzu Kubernetes Grid クラスタのノードと、スーパーバイザー 制御プレーン仮想マシンへの接続を提供します。Kubernetes 制御プレーン仮想マシンに接続を提供するワークロード ネットワークは、プライマリ ワークロード ネットワークと呼ばれます。各 スーパーバイザー にそれぞれ 1 つのプライマリ ワークロード ネットワークが必要です。スーパーバイザー に対して、分散ポート グループの 1 つをプライマリ ワークロード ネットワークとして指定する必要があります。

スーパーバイザー 上の Kubernetes 制御プレーン仮想マシンは、プライマリ ワークロード ネットワークに割り当てられた IP アドレス範囲から 3 つの IP アドレスを使用します。Tanzu Kubernetes Grid クラスタの各ノードには、この Tanzu Kubernetes Grid クラスタが実行されている名前空間で構成されたワークロード ネットワークのアドレス範囲から割り当てられた、それぞれ別の IP アドレスが割り当てられます。

ネットワーク要件

NSX Advanced Load Balancer には、次の 2 つのルーティング可能なサブネットが必要です。

- 管理ネットワーク。管理ネットワークには、NSX Advanced Load Balancer Controller（別名、コントローラ）が配置されています。管理ネットワークは、コントローラに vCenter Server、ESXi ホスト、および スーパーバイザー 制御プレーン ノードへの接続を提供します。このネットワークには、Avi サービス エンジンの管理インターフェイスが配置されます。このネットワークには、Distributed Switch と分散ポート グループが必要です。
- データ ネットワーク。Avi サービス エンジン（別名、サービス エンジン）のデータ インターフェイスはこのネットワークに接続されます。ロード バランサの仮想 IP アドレス (VIP) は、このネットワークから割り当てられます。このネットワークには、Distributed Switch と分散ポート グループが必要です。ロード バランサをインストールする前に、Distributed Switch と分散ポート グループを構成する必要があります。

IP アドレスの割り当て

コントローラとサービス エンジンは管理ネットワークに接続されます。NSX Advanced Load Balancer をインストールして構成する際に、各コントローラ仮想マシンのルーティング可能な固定 IP アドレスを指定します。

サービス エンジンでは DHCP を使用できます。DHCP を使用できない場合は、サービス エンジンの IP アドレス プールを構成できます。

コンピューティングの最小要件

次の表に、NSX Advanced Load Balancer を使用した Distributed Switch ネットワークのコンピューティングの最小要件を示します。ベスト プラクティスとして、管理ドメインとワークロード ドメインを分離することを検討してください。ワークロード ドメインは、ワークロードが実行される スーパーバイザー をホストします。管理ドメインは、vCenter Server などのすべての管理コンポーネントをホストします。

表 6-1. コンピューティングの最小要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8.0	小	2	21 GB	290 GB
ESXi ホスト 8.0	■ vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ 4 台の ESXi ホスト（クラスタごと）。 ホストは、vSphere DRS と HA が有効になっているクラスタに参加している必要があります。vSphere DRS は、完全自動化モードまたは一部自動化モードになっている必要があります。 **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB
NSX Advanced Load Balancer コントローラ	Enterprise 本番環境では、3 台の Avi Controller 仮想マシンによるクラスタをインストールすることを推奨します。HA 構成にするには、2 台以上のサービス エンジン仮想マシンが必要です。	4（小） 8（中） 24（大）	12 GB 24 GB 128 GB	128 GB 128 GB 128 GB
サービス エンジン	HA 構成にするには、2 台以上のサービス エンジン仮想マシンが必要です。	1	2 GB	15 GB

ネットワークの最小要件

次の表に、NSX Advanced Load Balancer を使用した vSphere ネットワークの最小ネットワーク要件を示します。

注： vSphere 7 スーパーバイザー による IPv6 クラスタの作成や、Tanzu Mission Control による IPv6 クラスタの登録はできません。NSX Advanced Load Balancer サービスは現在 IPv6 をサポートしていません。

表 6-2. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
物理ネットワークの MTU	1500	分散ポート グループの MTU サイズは 1500 以上にする必要があります。

表 6-3. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP) **注：** ワークロード ネットワークの DHCP 構成は、Distributed Switch スタックが構成された スーパーバイザーの スーパーバイザー サービス ではサポートされません。スーパーバイザー サービス を使用するには、固定 IP アドレスを使用してワークロード ネットワークを構成します。ただし、管理ネットワークには DHCP を使用できます。

表 6-4. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。
管理ネットワークのサブネット	1	管理ネットワークには、NSX Advanced Load Balancer Controller（別名、コントローラ）が配置されています。 また、サービス エンジン管理インターフェイスも接続されます。Controller は、このネットワーク内の vCenter Server および ESXi 管理 IP アドレスに接続する必要があります **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。

表 6-5. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere Distributed Switch	1	vSphere クラスタのすべてのホストが Distributed Switch に接続されている必要があります。
ワークロード ネットワーク	1	プライマリ ワークロード ネットワークとして構成する Distributed Switch には、1 つ以上の分散ポート グループを作成する必要があります。選択したトポロジによっては、名前空間のワークロード ネットワークと同じ分散ポート グループを使用することや、追加のポート グループを作成してワークロード ネットワークとして構成することができます。ワークロード ネットワークは次の要件を満たす必要があります。 ■ 任意のワークロード ネットワークと、NSX Advanced Load Balancer が仮想 IP アドレスの割り当てに使用するネットワークとの間でルーティングできること。 ■ スーパーバイザー 内のすべてのワークロード ネットワークで IP アドレス範囲の重複がないこと。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

表 6-6. ロード バランサ ネットワークの要件

NTP サーバおよび DNS サーバ	1	NSX Advanced Load Balancer Controller で vCenter Server と ESXi のホスト名が正しく解決されるようにするには、DNS サーバの IP アドレスが必要です。パブリック NTP サーバはデフォルトで使用されるため、NTP は省略可能です。
データ ネットワークのサブネット	1	NSX Advanced Load Balancer サービス エンジン（別名、サービス エンジン）のデータ インターフェイスはこのネットワークに接続されます。サービス エンジンの IP アドレス プールを構成します。ロード バランサの仮想 IP アドレス (VIP) は、このネットワークから割り当てられます。

表 6-6. ロード バランサ ネットワークの要件 （続き）

NSX Advanced Load Balancer Controller の IP アドレス	1 または 4	NSX Advanced Load Balancer Controller を単一ノードとしてデプロイする場合、その管理インターフェイス用に 1 つの固定 IP アドレスが必要です。 3 ノード クラスタの場合は、4 つの IP アドレスが必要です。各 NSX Advanced Load Balancer Controller 仮想マシンに 1 つ、クラスタ仮想 IP アドレスに 1 つです。これらの IP アドレスは、管理ネットワーク サブネットから取得する必要があります。
VIP IP アドレス管理の範囲	-	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。IP アドレスは、データ ネットワーク サブネットから取得する必要があります。スーパーバイザー クラスタごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

ポートとプロトコル

次の表に、NSX Advanced Load Balancer、vCenter Server とその他の vSphere IaaS control plane コンポーネント間の IP 接続を管理するために必要なプロトコルとポートを示します。

ソース	ターゲット	プロトコルとポート
NSX Advanced Load Balancer コントローラ	NSX Advanced Load Balancer Controller（クラスタ内）	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
サービス エンジン	HA のサービス エンジン	TCP 9001（VMware、LSC、NSX-T クラウド用）
サービス エンジン	NSX Advanced Load Balancer コントローラ	TCP 22 (SSH) TCP 8443 (HTTPS) UDP 123 (NTP)
Avi Controller	vCenter Server、ESXi、NSX-T Manager	TCP 443 (HTTPS)
スーパーバイザー制御プレーンノード (AKO)	NSX Advanced Load Balancer コントローラ	TCP 443 (HTTPS)

NSX Advanced Load Balancer のポートとプロトコルの詳細については、https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer を参照してください。

NSX を使用したクラスタ スーパーバイザー のデプロイの要件

NSX ネットワーク スタックを使用して、vSphere クラスタに vSphere IaaS control plane を構成するためのシステム要件を確認します。vSphere クラスタを スーパーバイザー として有効にすると、vSphere Zone が スーパーバイザー 用に自動的に作成されます。

これらの要件に加えて、NSX のデプロイに関するベスト プラクティスの詳細については、『NSX Reference Design Guide』を参照してください。

管理および Edge クラスタの最小限のコンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8	小	2	21 GB	290 GB
ESXi ホスト 8	2 台の ESXi ホスト	8	ホストあたり 64 GB	該当なし
NSX Manager	中	6	24 GB	300 GB
NSX Edge 1	大	8	32 GB	200 GB
NSX Edge 2	大	8	32 GB	200 GB

注： vSphere IaaS control plane を構成する vSphere クラスタに参加しているすべての ESXi ホストが、NSX トランスポート ノードとして準備されていることを確認します。詳細については、NSX ドキュメントの「トランスポート ノードとしての ESXi ホストの準備」と https://kb.vmware.com/s/article/95820 を参照してください。

ワークロード ドメイン クラスタの最小限のコンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vSphere クラスタ	■ 1 つの vSphere クラスタ ■ vSphere クラスタで vSphere DRS と HA が有効になっている。vSphere DRS は、完全自動化モードになっている必要があります。	該当なし	該当なし	該当なし
ESXi ホスト 8	■ vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ 4 台の ESXi ホスト **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB

ネットワーク要件

注： vSphere 8 スーパーバイザー による IPv6 クラスタの作成や、Tanzu Mission Control による IPv6 クラスタの登録はできません。

VMware 製品の相互運用性マトリックスで、サポート対象の NSX のバージョンを確認します。

表 6-7. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
物理ネットワークの MTU	1500	vSphere Distributed Switch ポート グループの MTU サイズは 1500 以上にする必要があります。
物理 NIC	vSAN が使用されている場合は、ホストあたり 2 つ以上の物理 NIC	Antrea CNI を使用し、最適な NSX パフォーマンスを得るには、参加している各 ESXi ホスト上の各物理 NIC で GENEVE カプセル化がサポートされていること、および GENEVE カプセル化を有効にすることが必要です。

表 6-8. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP)
イメージ レジストリ	1	サービスのレジストリへのアクセス。

表 6-9. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。

表 6-9. 管理ネットワークの要件 （続き）

コンポーネント	最小数	必要な構成
管理ネットワークのサブネット	1	ESXi ホストと、vCenter Server、NSX アプライアンス、および Kubernetes 制御プレーンとの間の管理トラフィックに使用されるサブネット。サブネットのサイズは次のようにする必要があります。 ■ ホストの VMkernel アダプタごとに 1 つの IP アドレス。 ■ vCenter Server アプライアンスに 1 つの IP アドレス。 ■ NSX Manager に 1 つまたは 4 つの IP アドレス。3 台のノードと 1 つの仮想 IP アドレス (VIP) の NSX Manager クラスタリングを実行する場合は 4 つです。 ■ Kubernetes 制御プレーンに 5 つの IP アドレス。3 台のノードそれぞれに 1 つずつ、仮想 IP アドレス用に 1 つ、クラスタのローリング アップグレード用に 1 つ。 **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。
管理ネットワークの VLAN	1	管理ネットワークのサブネットの VLAN ID。

表 6-10. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere ポッド CIDR 範囲	/23 プライベート IP アドレス	vSphere ポッド の IP アドレスを提供するプライベート CIDR 範囲。これらのアドレスは、Tanzu Kubernetes Grid クラスタ ノードにも使用されます。 クラスタごとに一意の vSphere ポッド CIDR 範囲を指定する必要があります。 **注：** vSphere ポッド の CIDR 範囲と、Kubernetes サービス アドレスの CIDR 範囲が重複しないようにする必要があります。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

表 6-10. ワークロード ネットワークの要件 （続き）

コンポーネント	最小数	必要な構成
出力方向 CIDR の範囲	/27 固定 IP アドレス	Kubernetes サービスの出力方向 IP アドレスを決定するプライベート CIDR 注釈。スーパーバイザー 内の名前空間ごとに 1 つの出力方向 IP アドレスのみが割り当てられます。出力方向 IP アドレスは、外部エンティティが名前空間内のサービスとの通信に使用するアドレスです。出力方向 IP アドレスの数によって、スーパーバイザー で保持できる出力方向ポリシーの数が制限されます。 最小値は /27 以上の CIDR です。たとえば、`10.174.4.96/27`。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
入力方向 CIDR	/27 固定 IP アドレス	入力方向の IP アドレスに使用されるプライベート CIDR 範囲。入力方向を使用すると、外部ネットワークから スーパーバイザー に送信される要求にトラフィック ポリシーを適用できます。入力方向 IP アドレスの数によって、クラスタで保持できる入力の数が制限されます。 最小値は /27 以上の CIDR です。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
名前空間ネットワーク範囲	1	サブネット/セグメントを作成し、ワークロードに IP アドレスを割り当てる 1 つ以上の IP CIDR。
名前空間サブネット プリフィックス	1	名前空間セグメント用に予約されるサブネットのサイズを指定するサブネット プリフィックス。デフォルトは 28 です。

表 6-11. NSX の要件

コンポーネント	最小数	必要な構成
VLAN	3	VLAN IP アドレスはトンネル エンドポイント (TEP) の IP アドレスです。ESXi ホスト TEP と Edge TEP はルーティング可能である必要があります。 VLAN IP アドレスが必要となるものは次のとおりです。 ■ ESXi ホスト VTEP ■ 固定 IP アドレスを使用する Edge VTEP ■ トランスポート ノードの Tier-0 ゲートウェイとアップリンク。 **注：** ESXi ホスト VTEP および Edge VTEP では、MTU サイズを 1,600 よりも大きくする必要があります。 ESXi ホストおよび NSX-T Edge ノードはトンネル エンドポイントとして機能し、各ホストおよび Edge ノードにトンネル エンドポイント (TEP) IP アドレスが割り当てられます。 ESXi ホストの TEP IP アドレスは Edge ノードの TEP IP アドレスとのオーバーレイ トンネルを確立するため、VLAN IP アドレスはルーティング可能である必要があります。 Tier-0 ゲートウェイへの North-South 接続を提供するには、追加の VLAN が必要です。 IP アドレス プールはクラスタ間で共有できます。ただし、ホスト オーバーレイの IP アドレス プール/VLAN を Edge オーバーレイの IP アドレス プール/VLAN と共有することはできません。 **注：** ホスト TEP と Edge TEP が異なる物理 NIC を使用している場合、同じ VLAN を使用できます。
Tier-0 アップリンクの IP アドレス	/24 プライベート IP アドレス	Tier 0 アップリンクに使用される IP サブネット。Tier 0 アップリンクの IP アドレスの要件は次のとおりです。 ■ 1 つの IP アドレス : Edge の冗長性を使用しない場合。 ■ 4 つの IP アドレス : BGP と Edge の冗長性を使用する場合。Edge ごとに 2 つの IP アドレス。 ■ 3 つの IP アドレス : スタティック ルートと Edge の冗長性を使用する場合。 Edge 管理の IP アドレス、サブネット、ゲートウェイ、アップリンクの IP アドレス、サブネット、ゲートウェイは一意である必要があります。

NSX および NSX Advanced Load Balancer を使用したクラスタ スーパーバイザー のデプロイの要件

NSX ネットワーク スタックを使用して、vSphere クラスタに vSphere IaaS control plane を構成するためのシステム要件を確認します。vSphere クラスタを スーパーバイザー として有効にすると、vSphere Zone が スーパーバイザー 用に自動的に作成されます。

NSX デプロイのオプション

NSX をデプロイする際のベスト プラクティスの詳細については、『NSX Reference Design Guide』を参照してください。

管理および Edge クラスタの最小限のコンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8	小	2	21 GB	290 GB
ESXi ホスト 8	2 台の ESXi ホスト	8	ホストあたり 64 GB	該当なし
NSX Manager	中	6	24 GB	300 GB
NSX Edge 1	大	8	32 GB	200 GB
NSX Edge 2	大	8	32 GB	200 GB
サービス エンジン仮想マシン	スーパーバイザー ごとに少なくとも 2 台のサービス エンジン仮想マシンがデプロイされます	1	2 GB	該当なし

注： vSphere IaaS control plane を構成する vSphere クラスタに参加しているすべての ESXi ホストが、NSX トランスポート ノードとして準備されていることを確認します。詳細については、NSX ドキュメントの「トランスポート ノードとしての ESXi ホストの準備」と https://kb.vmware.com/s/article/95820 を参照してください。

コントローラのシステム キャパシティの指定

デプロイ時にコントローラのシステム キャパシティを指定できます。システム キャパシティは、CPU、RAM、ディスクなどシステム リソースの割り当てに基づきます。割り当てるリソースの量はコントローラのパフォーマンスに影響します。

デプロイ タイプ	ノード数	推奨される割り当て - CPU	推奨される割り当て - メモリ	推奨される割り当て - ディスク
デモ/ユーザーによる評価	1	6	24 GB	128 GB

デモ用デプロイでは、単一のコントローラが適切です。すべての制御プレーン アクティビティとワークフロー、および分析に単一のコントローラが使用されます。

本番デプロイでは、3 ノードのクラスタが推奨されます。

詳細については、「NSX Advanced Load Balancer Controller のサイジング」を参照してください。

ワークロード ドメイン クラスタの最小限のコンピューティング要件

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vSphere クラスタ	■ 1 つの vSphere クラスタ ■ vSphere クラスタで vSphere DRS と HA が有効になっている。vSphere DRS は、完全自動化モードになっている必要があります。	該当なし	該当なし	該当なし
ESXi ホスト 8	■ vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 ■ vSAN を使用する場合：2 つ以上の物理 NIC を持つ 4 台の ESXi ホスト **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。使用されていない場合、スーパーバイザー の有効化が失敗することがあります。	8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB

ネットワーク要件

注： vSphere 8 スーパーバイザー による IPv6 クラスタの作成や、Tanzu Mission Control による IPv6 クラスタの登録はできません。

VMware 製品の相互運用性マトリックスで、サポート対象の NSX のバージョンを確認します。

表 6-12. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
物理ネットワークの MTU	1,700	vSphere Distributed Switch ポート グループの MTU サイズは 1,700 以上にする必要があります。
物理 NIC	vSAN が使用されている場合は、ホストあたり 2 つ以上の物理 NIC	Antrea CNI を使用し、最適な NSX パフォーマンスを得るには、参加している各 ESXi ホスト上の各物理 NIC で GENEVE カプセル化がサポートされていること、および GENEVE カプセル化を有効にすることが必要です。

表 6-13. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP)
イメージ レジストリ	1	サービスのレジストリへのアクセス。

表 6-14. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。

表 6-14. 管理ネットワークの要件 （続き）

コンポーネント	最小数	必要な構成
管理ネットワークのサブネット	1	ESXi ホストと、vCenter Server、NSX アプライアンス、および Kubernetes 制御プレーンとの間の管理トラフィックに使用されるサブネット。サブネットのサイズは次のようにする必要があります。 ■ ホストの VMkernel アダプタごとに 1 つの IP アドレス。 ■ vCenter Server アプライアンスに 1 つの IP アドレス。 ■ NSX Manager に 1 つまたは 4 つの IP アドレス。3 台のノードと 1 つの仮想 IP アドレス (VIP) の NSX Manager クラスタリングを実行する場合は 4 つです。 ■ Kubernetes 制御プレーンに 5 つの IP アドレス。3 台のノードそれぞれに 1 つずつ、仮想 IP アドレス用に 1 つ、クラスタのローリング アップグレード用に 1 つ。 **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。
管理ネットワークの VLAN	1	管理ネットワークのサブネットの VLAN ID。

表 6-15. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere ポッド CIDR 範囲	/23 プライベート IP アドレス	vSphere ポッド の IP アドレスを提供するプライベート CIDR 範囲。これらのアドレスは、Tanzu Kubernetes Grid クラスタ ノードにも使用されます。 クラスタごとに一意の vSphere ポッド CIDR 範囲を指定する必要があります。 **注：** vSphere ポッド の CIDR 範囲と、Kubernetes サービス アドレスの CIDR 範囲が重複しないようにする必要があります。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

表 6-15. ワークロード ネットワークの要件 （続き）

コンポーネント	最小数	必要な構成
出力方向 CIDR の範囲	/27 固定 IP アドレス	Kubernetes サービスの出力方向 IP アドレスを決定するプライベート CIDR 注釈。スーパーバイザー 内の名前空間ごとに 1 つの出力方向 IP アドレスのみが割り当てられます。出力方向 IP アドレスは、外部エンティティが名前空間内のサービスとの通信に使用するアドレスです。出力方向 IP アドレスの数によって、スーパーバイザー で保持できる出力方向ポリシーの数が制限されます。 最小値は /27 以上の CIDR です。たとえば、`10.174.4.96/27`。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
入力方向 CIDR	/27 固定 IP アドレス	入力方向の IP アドレスに使用されるプライベート CIDR 範囲。入力方向を使用すると、外部ネットワークから スーパーバイザー に送信される要求にトラフィック ポリシーを適用できます。入力方向 IP アドレスの数によって、クラスタで保持できる入力の数が制限されます。 最小値は /27 以上の CIDR です。 **注：** 出力方向 IP アドレスと入力方向 IP アドレスは重複できません。
名前空間ネットワーク範囲	1	サブネット/セグメントを作成し、ワークロードに IP アドレスを割り当てる 1 つ以上の IP CIDR。
名前空間サブネット プリフィックス	1	名前空間セグメント用に予約されるサブネットのサイズを指定するサブネット プリフィックス。デフォルトは 28 です。

表 6-16. NSX の要件

コンポーネント	最小数	必要な構成
VLAN	3	VLAN IP アドレスはトンネル エンドポイント (TEP) の IP アドレスです。ESXi ホスト TEP と Edge TEP はルーティング可能である必要があります。 VLAN IP アドレスが必要となるものは次のとおりです。 ■ ESXi ホスト VTEP ■ 固定 IP アドレスを使用する Edge VTEP ■ トランスポート ノードの Tier-0 ゲートウェイとアップリンク。 **注：** ESXi ホスト VTEP および Edge VTEP では、MTU サイズを 1,600 よりも大きくする必要があります。 ESXi ホストおよび NSX-T Edge ノードはトンネル エンドポイントとして機能し、各ホストおよび Edge ノードにトンネル エンドポイント (TEP) IP アドレスが割り当てられます。 ESXi ホストの TEP IP アドレスは Edge ノードの TEP IP アドレスとのオーバーレイ トンネルを確立するため、VLAN IP アドレスはルーティング可能である必要があります。 Tier-0 ゲートウェイへの North-South 接続を提供するには、追加の VLAN が必要です。 IP アドレス プールはクラスタ間で共有できます。ただし、ホスト オーバーレイの IP アドレス プール/VLAN を Edge オーバーレイの IP アドレス プール/VLAN と共有することはできません。 **注：** ホスト TEP と Edge TEP が異なる物理 NIC を使用している場合、同じ VLAN を使用できます。
Tier-0 アップリンクの IP アドレス	/24 プライベート IP アドレス	Tier 0 アップリンクに使用される IP サブネット。Tier 0 アップリンクの IP アドレスの要件は次のとおりです。 ■ 1 つの IP アドレス：Edge の冗長性を使用しない場合。 ■ 4 つの IP アドレス：BGP と Edge の冗長性を使用する場合。Edge ごとに 2 つの IP アドレス。 ■ 3 つの IP アドレス：スタティック ルートと Edge の冗長性を使用する場合。 Edge 管理の IP アドレス、サブネット、ゲートウェイ、アップリンクの IP アドレス、サブネット、ゲートウェイは一意である必要があります。

表 6-17. ロード バランサ ネットワークの要件

NTP サーバおよび DNS サーバ	1	NSX Advanced Load Balancer Controller で vCenter Server と ESXi のホスト名が正しく解決されるようにするには、DNS サーバの IP アドレスが必要です。パブリック NTP サーバはデフォルトで使用されるため、NTP は省略可能です。
データ ネットワークのサブネット	1	NSX Advanced Load Balancer サービス エンジン（別名、サービス エンジン）のデータ インターフェイスはこのネットワークに接続されます。サービス エンジンの IP アドレス プールを構成します。ロード バランサの仮想 IP アドレス (VIP) は、このネットワークから割り当てられます。
NSX Advanced Load Balancer Controller の IP アドレス	1 または 4	NSX Advanced Load Balancer Controller を単一ノードとしてデプロイする場合、その管理インターフェイス用に 1 つの固定 IP アドレスが必要です。 3 ノード クラスタの場合は、4 つの IP アドレスが必要です。各 NSX Advanced Load Balancer Controller 仮想マシンに 1 つ、クラスタ仮想 IP アドレスに 1 つです。これらの IP アドレスは、管理ネットワーク サブネットから取得する必要があります。
VIP IP アドレス管理の範囲	-	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。IP アドレスは、データ ネットワーク サブネットから取得する必要があります。スーパーバイザー クラスタごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

ポートとプロトコル

次の表に、NSX Advanced Load Balancer、vCenter Server とその他の vSphere IaaS control plane コンポーネント間の IP 接続を管理するために必要なプロトコルとポートを示します。

ソース	ターゲット	プロトコルとポート
NSX Advanced Load Balancer コントローラ	NSX Advanced Load Balancer Controller（クラスタ内）	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
サービス エンジン	HA のサービス エンジン	TCP 9001（VMware、LSC、NSX-T クラウド用）
サービス エンジン	NSX Advanced Load Balancer コントローラ	TCP 22 (SSH) TCP 8443 (HTTPS) UDP 123 (NTP)

ソース	ターゲット	プロトコルとポート
Avi Controller	vCenter Server、ESXi、NSX-T Manager	TCP 443 (HTTPS)
スーパーバイザー制御プレーンノード (AKO)	NSX Advanced Load Balancer コントローラ	TCP 443 (HTTPS)

NSX Advanced Load Balancer のポートとプロトコルの詳細については、https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer を参照してください。

Distributed Switch ネットワークと HAProxy ロード バランサを使用したクラスタ スーパーバイザー のデプロイの要件

Distributed Switch ネットワーク スタックと HAProxy ロード バランサを使用して vSphere クラスタを スーパーバイザー としてセットアップするためのシステム要件を確認します。vSphere クラスタを スーパーバイザー として有効にすると、vSphere Zone が スーパーバイザー 用に自動的に作成されます。

コンピューティングの最小要件

ベスト プラクティスとして、管理ドメインとワークロード ドメインを分離することを検討してください。ワークロード ドメインは、ワークロードが実行される スーパーバイザー をホストします。管理ドメインは、vCenter Server などのすべての管理コンポーネントをホストします。

システム	最小デプロイ サイズ	CPU	メモリ	ストレージ
vCenter Server 8.0	小	2	21 GB	290 GB
ESXi ホスト 8.0	vSAN を使用しない場合：3 台の ESXi ホストと、ホストあたり 1 つの固定 IP アドレス。 vSAN を使用する場合：2 つ以上の物理 NIC を持つ 4 台の ESXi ホスト ホストは、vSphere DRS と HA が有効になっているクラスタに参加している必要があります。vSphere DRS は、完全自動化モードまたは一部自動化モードになっている必要があります。 **注：** クラスタに参加するホストの名前に小文字が使用されていることを確認します。この条件に該当しない場合は、ワークロード管理のためのクラスタの有効化が失敗する場合があります。	8	ホストあたり 64 GB	該当なし
Kubernetes 制御プレーンの仮想マシン	3	4	16 GB	16 GB

ネットワークの最小要件

注： vSphere 8 スーパーバイザー による IPv6 クラスタの作成や、Tanzu Mission Control による IPv6 クラスタの登録はできません。

表 6-18. 物理ネットワークの要件

コンポーネント	最小数	必要な構成
物理ネットワークの MTU	1500	分散ポート グループの MTU サイズは 1500 以上にする必要があります。

表 6-19. 一般的なネットワークの要件

コンポーネント	最小数	必要な構成
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 管理ネットワークの場合、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなどのすべての IP アドレスは、DHCP サーバから自動的に取得されます。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP) **注：** ワークロード ネットワークの DHCP 構成は、Distributed Switch スタックが構成された スーパーバイザー の スーパーバイザー サービス ではサポートされません。スーパーバイザー サービス を使用するには、固定 IP アドレスを使用してワークロード ネットワークを構成します。ただし、管理ネットワークには DHCP を使用できます。

表 6-20. 管理ネットワークの要件

コンポーネント	最小数	必要な構成
Kubernetes 制御プレーン仮想マシンの固定 IP アドレス	5 つのアドレスのブロック	管理ネットワークから スーパーバイザー 内の Kubernetes 制御プレーン仮想マシンに割り当てられる、連続する 5 つの固定 IP アドレスのブロック。
管理トラフィック ネットワーク	1	ESXi ホスト、vCenter Server、スーパーバイザー、およびロード バランサにルーティング可能な管理ネットワーク。

表 6-20. 管理ネットワークの要件 （続き）

コンポーネント	最小数	必要な構成
管理ネットワークのサブネット	1	ESXi ホストおよび vCenter Server と Kubernetes 制御プレーンとの間の管理トラフィックに使用されるサブネット。サブネットのサイズは次のようにする必要があります。 ■ ホストの VMkernel アダプタごとに 1 つの IP アドレス。 ■ vCenter Server アプライアンスに 1 つの IP アドレス。 ■ Kubernetes 制御プレーンに 5 つの IP アドレス。3 台のノードそれぞれに 1 つずつ、仮想 IP アドレス用に 1 つ、クラスタのローリング アップグレード用に 1 つ。 **注：** 管理ネットワークとワークロード ネットワークは異なるサブネット上に配置する必要があります。管理ネットワークとワークロード ネットワークに同じサブネットを割り当てることはできないため、システム エラーや問題が発生することがあります。
管理ネットワークの VLAN	1	管理ネットワークのサブネットの VLAN ID。

表 6-21. ワークロード ネットワークの要件

コンポーネント	最小数	必要な構成
vSphere Distributed Switch	1	vSphere クラスタのすべてのホストが Distributed Switch に接続されている必要があります。
ワークロード ネットワーク	1	プライマリ ワークロード ネットワークとして構成する Distributed Switch には、1 つ以上の分散ポート グループを作成する必要があります。選択したトポロジによっては、名前空間のワークロード ネットワークと同じ分散ポート グループを使用することや、追加のポート グループを作成してワークロード ネットワークとして構成することができます。ワークロード ネットワークは次の要件を満たす必要があります。 ■ 任意のワークロード ネットワークと、HAProxy が仮想 IP アドレスの割り当てに使用するネットワークとの間でルーティングできること。 ■ スーパーバイザー 内のすべてのワークロード ネットワークで IP アドレス範囲の重複がないこと。 **重要：** ワークロード ネットワークは、管理ネットワークとは別のサブネットに配置してください。
Kubernetes サービスの CIDR 範囲	/16 プライベート IP アドレス	Kubernetes サービスに IP アドレスを割り当てるためのプライベート CIDR 範囲。スーパーバイザー ごとに一意の Kubernetes サービス CIDR 範囲を指定する必要があります。

表 6-22. ロード バランサ ネットワークの要件

HAProxy ロード バランサ	1	vCenter Server インスタンスで構成された HAProxy ロード バランサのインスタンス。 ■ 1 つの HAProxy インスタンスが複数の スーパーバイザー で使用されている場合、すべての スーパーバイザー のすべてのワークロード ネットワークとの間で、トラフィックをルーティングできる必要があります。 ■ HAProxy を使用するすべての スーパーバイザー のワークロード ネットワークにまたがる IP アドレス範囲は、重複しないようにする必要があります。 ■ HAProxy が仮想 IP アドレスを割り当てるために使用するネットワークは、この HAProxy が接続されているすべての スーパーバイザー で使用されるワークロード ネットワークにルーティング可能である必要があります。
仮想サーバの IP アドレス範囲	1	仮想 IP アドレスの専用 IP アドレス範囲。HAProxy 仮想マシンは、この仮想 IP アドレス範囲の唯一の所有者である必要があります。この範囲は、どの スーパーバイザー が所有するワークロード ネットワークに割り当てられた IP アドレス範囲とも重複が許されません。また、管理ネットワークと同じサブネット上にあってはなりません。

コンポーネント	最小数	必要な構成
NTP サーバおよび DNS サーバ	1	vCenter Server で使用できる DNS サーバおよび NTP サーバ。 **注：** すべての ESXi ホストおよび vCenter Server で NTP を構成します。
DHCP サーバ	1	オプション。管理ネットワークとワークロード ネットワークの IP アドレスおよびフローティング IP アドレスを自動的に取得するように DHCP サーバを構成します。DHCP サーバはクライアント識別子をサポートし、互換性のある DNS サーバ、DNS 検索ドメイン、および NTP サーバを提供する必要があります。 DHCP 構成は、スーパーバイザー で使用されます。ロード バランサで管理を行うには、固定 IP アドレスが必要になる場合があります。DHCP スコープは、これらの固定 IP アドレスと重複しないようにしてください。DHCP は仮想 IP アドレスには使用されません。(VIP)